The Future of Truth and Misinformation Online

Experts are evenly split on whether the coming decade will see a reduction in false and misleading narratives online. Those forecasting improvement place their hopes in technological fixes and in societal solutions. Others think the dark side of human nature is aided more than stifled by technology.

BY *Janna Anderson and Lee Rainie*

About Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. The center conducts public opinion polling, demographic research, content analysis and other data-driven social science research. It studies U.S. politics and policy; journalism and media; internet, science and technology; religion and public life; Hispanic trends; global attitudes and trends; and U.S. social and demographic trends. All of the Center's reports are available at www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts, its primary funder.

For this project, Pew Research Center worked with Elon University's Imagining the Internet Center, which helped conceive the research and collect and analyze the data.

© Pew Research Center 2017

The Future of Truth and Misinformation Online

Experts are evenly split on whether the coming decade will see a reduction in false and misleading narratives online. Those forecasting improvement place their hopes in technological fixes and in societal solutions. Others think the dark side of human nature is aided more than stifled by technology.

In late 2016, Oxford Dictionaries selected "post-truth" as the word of the year, defining it as "relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief."

The 2016 Brexit vote in the United Kingdom and the tumultuous U.S. presidential election highlighted how the digital age has affected news and cultural narratives. New information platforms feed the ancient instinct people have to find information that syncs with their perspectives: A 2016 study that analyzed 376 million Facebook users' interactions with over 900 news outlets found that people tend to seek information that aligns with their views.

This makes many vulnerable to accepting and acting on misinformation. For instance, after fake news stories in June 2017 reported Ethereum's founder Vitalik Buterin had died in a car crash its market value was reported to have dropped by $4 billion.

When BBC Future Now interviewed a panel of 50 experts in early 2017 about the "grand challenges we face in the 21st century" many named the breakdown of trusted information sources. "The major new challenge in reporting news is the new shape of truth," said Kevin Kelly, co-founder of Wired magazine. "Truth is no longer dictated by authorities, but is networked by peers. For every fact there is a counterfact and all these counterfacts and facts look identical online, which is confusing to most people."

Americans worry about that: A Pew Research Center study conducted just after the 2016 election found 64% of adults believe fake news stories cause a great deal of confusion and 23% said they had shared fabricated political stories themselves – sometimes by mistake and sometimes intentionally.

The question arises, then: What will happen to the online information environment in the coming decade? In summer 2017, Pew Research Center and Elon University's Imagining the

Internet Center conducted a large canvassing of technologists, scholars, practitioners, strategic thinkers and others, asking them to react to this framing of the issue:

> *The rise of "fake news" and the proliferation of doctored narratives that are spread by humans and bots online are challenging publishers and platforms. Those trying to stop the spread of false information are working to design technical and human systems that can weed it out and minimize the ways in which bots and other schemes spread lies and misinformation.*
>
> *The question: <u>In the next 10 years, will trusted methods emerge to block false narratives and allow the most accurate information to prevail in the overall information ecosystem? Or will the quality and veracity of information online deteriorate due to the spread of unreliable, sometimes even dangerous, socially destabilizing ideas?</u>*

Respondents were then asked to choose one of the following answer options:

> The information environment **will improve** – In the next 10 years, on balance, the information environment will be IMPROVED by changes that reduce the spread of lies and other misinformation online.
>
> The information environment **will NOT improve** – In the next 10 years, on balance, the information environment will NOT BE improved by changes designed to reduce the spread of lies and other misinformation online

Some 1,116 responded to this nonscientific canvassing: **51**% chose the option that the information environment will not improve, and **49%** said the information environment will improve. (See "About this canvassing of experts" for details about this sample.) Participants were next asked to explain their answers. This report concentrates on these follow-up responses.

Their reasoning revealed a wide range of opinions about the nature of these threats and the most likely solutions required to resolve them. But the overarching and competing themes were clear: Those who do not think things will improve felt that humans mostly shape technology advances to their own, not-fully-noble purposes and that bad actors with bad motives will thwart the best efforts of technology innovators to remedy today's problems.

And those who are most hopeful believed that technological fixes can be implemented to bring out the better angels guiding human nature.

More specifically, the 51% of these experts who expect things will _not improve_ generally cited two reasons:

The fake news ecosystem preys on some of our deepest human instincts: Respondents said humans' primal quest for success and power – their "survival" instinct – will continue to degrade the online information environment in the next decade. They predicted that manipulative actors will use new digital tools to take advantage of humans' inbred preference for comfort and convenience and their craving for the answers they find in reinforcing echo chambers.

We can't contend with the pace of technological change: These respondents said the rising speed, reach and efficiencies of the internet and emerging online applications will magnify these human tendencies and that technology-based solutions will not be able to overcome them. They predicted a future information landscape in which fake information crowds out reliable information. Some even foresaw a world in which widespread information scams and mass manipulation cause broad swathes of public to simply give up on being informed participants in civic life.

The 49% of these experts who expect things to _improve_ generally inverted that reasoning:

Technology can help fix these problems: These respondents said the rising speed, reach and efficiencies of the internet, apps and platforms can be harnessed to rein in fake news and misinformation campaigns. Some predicted better methods will arise to create and promote trusted, fact-based news sources.

It is also human nature to come together and fix problems: The hopeful experts in this canvassing took the view that people have always adapted to change and that this current wave of challenges will also be overcome. They noted that misinformation and bad actors have always existed but have eventually been marginalized by smart people and processes. They expect well-meaning actors will work together to find ways to enhance the information environment. They also believe better information literacy among citizens will enable people to judge the veracity of material content and eventually raise the tone of discourse.

The majority of participants in this canvassing wrote detailed elaborations on their views. Some chose to have their names connected to their answers; others opted to respond

anonymously. These findings do not represent all possible points of view, but they do reveal a wide range of striking observations.

Respondents collectively articulated several major themes tied to those insights and explained in the sections below the following graphic. Several longer additional sets of responses tied to these themes follow that summary.

The next section of this report presents an overview of the themes found among the written responses, including a small selection of representative quotes supporting each point. Some comments are lightly edited for style or length.

Major themes on the future of the online information environment

THINGS WILL NOT IMPROVE

Theme 1 **The information environment *will not* improve: The problem is human nature**

- More people = more problems. The internet's continuous growth and accelerating innovation allow more people and artificial intelligence (AI) to create and instantly spread manipulative narratives
- Humans are by nature selfish, tribal, gullible convenience seekers who put the most trust in that which seems familiar
- In existing economic, political and social systems, the powerful corporate and government leaders most able to improve the information environment profit most when it is in turmoil
- Human tendencies and infoglut drive people apart and make it harder for them to agree on "common knowledge." That makes healthy debate difficult and destabilizes trust. The fading of news media contributes to the problem
- A small segment of society will find, use and perhaps pay a premium for information from reliable sources. Outside of this group "chaos will reign" and a worsening digital divide will develop

Theme 2 **The information environment *will not* improve because technology will create new challenges that can't or won't be countered effectively and at scale**

- Those generally acting for themselves and not the public good have the advantage, and they are likely to stay ahead in the information wars
- Weaponized narratives and other false content will be magnified by social media, online filter bubbles and AI
- The most effective tech solutions to misinformation will endanger people's dwindling privacy options, and they are likely to limit free speech and remove the ability for people to be anonymous online

THINGS WILL IMPROVE

Theme 3 **The information environment *will* improve because technology will help label, filter or ban misinformation and thus upgrade the public's ability to judge the quality and veracity of content**

- Likely tech-based solutions include adjustments to algorithmic filters, browsers, apps and plug-ins and the implementation of "trust ratings"
- Regulatory remedies could include software liability law, required identities and the unbundling of social networks like Facebook

Theme 4 **The information environment *will* improve, because people will adjust and correct**

- Misinformation has always been with us and people have found ways to lessen its impact. The problems will become more manageable as people become more adept at sorting through material
- Crowdsourcing will work to highlight verified facts and block those who propagate lies and propaganda. Some also have hopes for distributed ledgers (blockchain)

MAJOR PROGRAMS ARE NECESSARY

Theme 5 **Tech can't win the battle. The public must fund and support the production of objective, accurate information. It must also elevate information literacy to be a primary goal of education**

- Funding and support must be directed to the restoration of a well-fortified, ethical and trusted public press
- Elevate information literacy: It must become a primary goal at all levels of education

PEW RESEARCH CENTER and ELON UNIVERSITY'S IMAGINING THE INTERNET CENTER

Theme 1: The information environment will not improve: The problem is human nature

Most respondents who expect the environment to worsen said human nature is at fault. For instance, **Christian H. Huitema**, former president of the Internet Architecture Board, commented, "The quality of information will not improve in the coming years, because technology can't improve human nature all that much."

These experts predicted that the problem of misinformation will be amplified because the worst side of human nature is magnified by bad actors using advanced online tools at internet speed on a vast scale.

Tom Rosenstiel, author, director of the American Press Institute and senior fellow at the Brookings Institution, commented, "Whatever changes platform companies make, and whatever innovations fact checkers and other journalists put in place, those who want to deceive will adapt to them. Misinformation is not like a plumbing problem you fix. It is a social condition, like crime, that you must constantly monitor and adjust to. Since as far back as the era of radio and before, as Winston Churchill said, 'A lie can go around the world before the truth gets its pants on.'"

Michael J. Oghia, an author, editor and journalist based in Europe, said he expects a worsening of the information environment due to five things: "1) The spread of misinformation and hate; 2) Inflammation, sociocultural conflict and violence; 3) The breakdown of socially accepted/agreed-upon knowledge and what constitutes 'fact'; 4) A new digital divide of those subscribed (and ultimately controlled) by misinformation and those who are 'enlightened' by information based on reason, logic, scientific inquiry and critical thinking; 5) Further divides between communities, so that as we are more connected we are farther apart. And many others."

Leah Lievrouw, professor in the department of information studies at the University of California, Los Angeles, observed, "So many players and interests see online information as a uniquely powerful shaper of individual action and public opinion in ways that serve their economic or political interests (marketing, politics, education, scientific controversies, community identity and solidarity, behavioral 'nudging,' etc.). These very diverse players would likely oppose (or try to subvert) technological or policy interventions or other attempts to insure the quality, and especially the disinterestedness, of information."

Subtheme: More people = more problems. The internet's continuous growth and accelerating innovation allow more people and artificial intelligence (AI) to create and instantly spread manipulative narratives

While propaganda and the manipulation of the public via falsehoods is a tactic as old as the human race, many of these experts predicted that the speed, reach and low cost of online communication plus continuously emerging innovations will magnify the threat level significantly. A **professor at a Washington, D.C.-area university** said, "It is nearly impossible to implement solutions at scale – the attack surface is too large to be defended successfully."

Jerry Michalski, futurist and founder of REX, replied, "The trustworthiness of our information environment will decrease over the next decade because: 1) It is inexpensive and easy for bad actors to act badly; 2) Potential technical solutions based on strong ID and public voting (for example) won't quite solve the problem; and 3) real solutions based on actual trusted relationships will take time to evolve – likely more than a decade."

An **institute director and university professor** said, "The internet is the 21st century's threat of a 'nuclear winter,' and there's no equivalent international framework for nonproliferation or disarmament. The public can grasp the destructive power of nuclear weapons in a way they will never understand the utterly corrosive power of the internet to civilized society, when there is no reliable mechanism for sorting out what people can believe to be true or false."

Bob Frankston, internet pioneer and software innovator, said, "I always thought that 'Mein Kampf' could be countered with enough information. Now I feel that people will tend to look for confirmation of their biases and the radical transparency will not shine a cleansing light."

David Harries, associate executive director for Foresight Canada, replied, "More and more, history is being written, rewritten and corrected, because more and more people have the ways and means to do so. Therefore there is ever more information that competes for attention, for credibility and for influence. The competition will complicate and intensify the search for veracity. Of course, many are less interested in veracity than in winning the competition."

Glenn Edens, CTO for technology reserve at PARC, a Xerox company, commented, "Misinformation is a two-way street. Producers have an easy publishing platform to reach

wide audiences and those audiences are flocking to the sources. The audiences typically are looking for information that fits their belief systems, so it is a really tough problem."

Subtheme: Humans are by nature selfish, tribal, gullible convenience-seekers who put the most trust in that which seems familiar

The respondents who supported this view noted that people's actions – from consciously malevolent and power-seeking behaviors to seemingly more benign acts undertaken for comfort or convenience – will work to undermine a healthy information environment.

An **executive consultant based in North America** wrote, "It comes down to motivation: There is no market for the truth. The public isn't motivated to seek out verified, vetted information. They are happy hearing what confirms their views. And people can gain more creating fake information (both monetary and in notoriety) than they can keeping it from occurring."

Serge Marelli, an IT professional who works on and with the Net, wrote, "As a group, humans are 'stupid.' It is 'group mind' or a 'group phenomenon' or, as George Carlin said, 'Never underestimate the power of stupid people in large groups.' Then, you have Kierkegaard, who said, 'People demand freedom of speech as a compensation for the freedom of thought which they seldom use.' And finally, Euripides said, 'Talk sense to a fool and he calls you foolish.'"

Starr Roxanne Hiltz, distinguished professor of information systems and co-author of the visionary 1970s book "The Network Nation," replied, "People on systems like Facebook are increasingly forming into 'echo chambers' of those who think alike. They will keep unfriending those who don't, and passing on rumors and fake news that agrees with their point of view. When the president of the U.S. frequently attacks the traditional media and anybody who does not agree with his 'alternative facts,' it is not good news for an uptick in reliable and trustworthy facts circulating in social media."

Nigel Cameron, a technology and futures editor and president of the Center for Policy on Emerging Technologies, said, "Human nature is not EVER going to change (though it may, of course, be manipulated). And the political environment is bad."

Ian O'Byrne, assistant professor at the College of Charleston, replied, "Human nature will take over as the salacious is often sexier than facts. There are multiple information streams, public and private, that spread this information online. We can also not trust the businesses

and industries that develop and facilitate these digital texts and tools to make changes that will significantly improve the situation."

Greg Swanson, media consultant with ITZonTarget, noted, "The sorting of reliable versus fake news requires a trusted referee. It seems unlikely that government can play a meaningful role as this referee. We are too polarized. And we have come to see the television news teams as representing divergent points of view, and, depending on your politics, the network that does not represent your views is guilty of 'fake news.' It is hard to imagine a fair referee that would be universally trusted."

Richard Lachmann, professor of sociology at the State University of New York atAlbany, replied, "Even though systems [that] flag unreliable information can and will be developed, internet users have to be willing to take advantage of those warnings. Too many Americans will live in political and social subcultures that will champion false information and encourage use of sites that present such false information."

There were also those among these expert respondents who said inequities, perceived and real, are at the root of much of the misinformation being produced.

A **professor at MIT** observed, "I see this as problem with a socioeconomic cure: Greater equity and justice will achieve much more than a bot war over facts. Controlling 'noise' is less a technological problem than a human problem, a problem of belief, of ideology. Profound levels of ungrounded beliefs about things both sacred and profane existed before the branding of 'fake news.' Belief systems – not 'truths' – help to cement identities, forge relationships, explain the unexplainable."

Julian Sefton-Green, professor of new media education at Deakin University in Australia, said, "The information environment is an extension of social and political tensions. It is impossible to make the information environment a rational, disinterested space; it will always be susceptible to pressure."

A **respondent affiliated with Harvard University's Berkman Klein Center for Internet & Society** wrote, "The democratization of publication and consumption that the networked sphere represents is too expansive for there to be any meaningful improvement possible in terms of controlling or labeling information. People will continue to cosset their own cognitive biases."

Subtheme: In existing economic, political and social systems, the powerful corporate and government leaders most able to improve the information environment profit most when it is in turmoil

A large number of respondents said the interests of the most highly motivated actors, including those in the worlds of business and politics, are generally not motivated to "fix" the proliferation of misinformation. Those players will be a key driver in the worsening of the information environment in the coming years and/or the lack of any serious attempts to effectively mitigate the problem.

Scott Shamp, a dean at Florida State University, commented, "Too many groups gain power through the proliferation of inaccurate or misleading information. When there is value in misinformation, it will rule."

Alex "Sandy" Pentland, member of the U.S. National Academy of Engineering and the World Economic Forum, commented, "We know how to dramatically improve the situation, based on studies of political and similar predictions. What we don't know is how to make it a thriving business. The current [information] models are driven by clickbait, and that is not the foundation of a sustainable economic model."

Stephen Downes, researcher with the National Research Council of Canada, wrote, "Things will not improve. There is too much incentive to spread disinformation, fake news, malware and the rest. Governments and organizations are major actors in this space."

An **anonymous respondent** said, "Actors can benefit socially, economically, politically by manipulating the information environment. As long as these incentives exist, actors will find a way to exploit them. These benefits are not amenable to technological resolution as they are social, political and cultural in nature. Solving this problem will require larger changes in society."

A number of respondents mentioned market capitalism as a primary obstacle to improving the information environment. A **professor based in North America** said, "[This] is a capitalist system. The information that will be disseminated will be biased, based on monetary interests."

Seth Finkelstein, consulting programmer and winner of the Electronic Freedom Foundation's Pioneer Award, commented, "Virtually all the structural incentives to spread misinformation seem to be getting worse."

A **data scientist based in Europe** wrote, "The information environment is built on the top of telecommunication infrastructures and services developed following the free-market ideology, where 'truth' or 'fact' are only useful as long as they can be commodified as market products."

Zbigniew Łukasiak, a business leader based in Europe, wrote, "Big political players have just learned how to play this game. I don't think they will put much effort into eliminating it."

A **vice president for public policy at one of the world's foremost entertainment and media companies** commented, "The small number of dominant online platforms do not have the skills or ethical center in place to build responsible systems, technical or procedural. They eschew accountability for the impact of their inventions on society and have not developed any of the principles or practices that can deal with the complex issues. They are like biomedical or nuclear technology firms absent any ethics rules or ethics training or philosophy. Worse, their active philosophy is that assessing and responding to likely or potential negative impacts of their inventions is both not theirs to do and even shouldn't be done."

Patricia Aufderheide, professor of communications and founder of the Center for Media and Social Impact at American University, said, "Major interests are not invested enough in reliability to create new business models and political and regulatory standards needed for the shift. … Overall there are powerful forces, including corporate investment in surveillance-based business models, that create many incentives for unreliability, 'invisible handshake' agreements with governments that militate against changing surveillance models, international espionage at a governmental and corporate level in conjunction with mediocre cryptography and poor use of white hat hackers, poor educational standards in major industrial countries such as the U.S., and fundamental weaknesses in the U.S. political/electoral system that encourage exploitation of unreliability. It would be wonderful to believe otherwise, and I hope that other commentators will be able to convince me otherwise."

James Schlaffer, an assistant professor of economics, commented, "Information is curated by people who have taken a step away from the objectivity that was the watchword of journalism. Conflict sells, especially to the opposition party, therefore the opposition news agency will be incentivized to push a narrative and agenda. Any safeguards will appear as a way to further control narrative and propagandize the population."

Subtheme: Human tendencies and infoglut drive people apart and make it harder for them to agree on 'common knowledge.' That makes healthy debate difficult and destabilizes trust. The fading of news media contributes to the problem

Many respondents expressed concerns about how people's struggles to find and apply accurate information contribute to a larger social and political problem: There is a growing deficit in commonly accepted facts or some sort of cultural "common ground." Why has this happened? They cited several reasons:

- Online echo chambers or silos divide people into separate camps, at times even inciting them to express anger and hatred at a volume not seen in previous communications forms.
- Information overload crushes people's attention spans. Their coping mechanism is to turn to entertainment or other lighter fare.
- High-quality journalism has been decimated due to changes in the attention economy.

They said these factors and others make it difficult for many people in the digital age to create and come to share the type of "common knowledge" that undergirds better and more-responsive public policy. A share of respondents said a lack of commonly shared knowledge leads many in society to doubt the reliability of everything, causing them to simply drop out of civic participation, depleting the number of active and informed citizens.

Jamais Cascio, distinguished fellow at the Institute for the Future, noted, "The power and diversity of very low-cost technologies allowing unsophisticated users to create believable 'alternative facts' is increasing rapidly. It's important to note that the goal of these tools is not necessarily to create consistent and believable alternative facts, but to create plausible levels of doubt in actual facts. The crisis we face about 'truth' and reliable facts is predicated less on the ability to get people to believe the *wrong* thing as it is on the ability to get people to *doubt* the right thing. The success of Donald Trump will be a flaming signal that this strategy works, alongside the variety of technologies now in development (and early deployment) that can exacerbate this problem. In short, it's a successful strategy, made simpler by more powerful information technologies."

Philip J. Nickel, lecturer at Eindhoven University of Technology in the Netherlands, said, "The decline of traditional news media and the persistence of closed social networks will not change in the next 10 years. These are the main causes of the deterioration of a public domain of shared facts as the basis for discourse and political debate."

Kenneth Sherrill, professor emeritus of political science at Hunter College, City University of New York, predicted, "Disseminating false rumors and reports will become easier. The proliferation of sources will increase the number of people who don't know who or what they trust. These people will drop out of the normal flow of information. Participation will decline as more and more citizens become unwilling/unable to figure out which information sources are reliable."

What is truth? What is a fact? Who gets to decide? And can most people agree to trust anything as "common knowledge"? A number of respondents challenged the idea that any individuals, groups or technology systems could or should "rate" information as credible, factual, true or not.

An **anonymous respondent** observed, "Whatever is devised will not be seen as impartial; some things are not black and white; for other situations, facts brought up to come to a conclusion are different that other facts used by others in a situation. Each can have real facts, but it is the facts that are gathered that matter in coming to a conclusion; who will determine what facts will be considered or what is even considered a fact."

A **research assistant at MIT** noted, "'Fake' and 'true' are not as binary as we would like, and – combined with an increasingly connected and complex digital society – it's a challenge to manage the complexity of social media without prescribing a narrative as 'truth.'"

An **internet pioneer and longtime leader at ICANN** said, "There is little prospect of a forcing factor that will emerge that will improve the 'truthfulness' of information in the internet."

A **vice president for stakeholder engagement** said, "Trust networks are best established with physical and unstructured interaction, discussion and observation. Technology is reducing opportunities for such interactions and disrupting human discourse, while giving the 'feeling' that we are communicating more than ever."

Subtheme: A small segment of society will find, use and perhaps pay a premium for information from reliable sources. Outside of this group 'chaos will reign' and a worsening digital divide will develop

Some respondents predicted that a larger digital divide will form. Those who pursue more-accurate information and rely on better-informed sources will separate from those who are not selective enough or who do not invest either the time or the money in doing so.

Alejandro Pisanty, a professor at UNAM, the National University of Mexico, and longtime internet policy leader, observed, "Overall, at least a part of society will value trusted information and find ways to keep a set of curated, quality information resources. This will use a combination of organizational and technological tools but above all, will require a sharpened sense of good judgment and access to diverse, including rivalrous, sources. Outside this, chaos will reign."

Alexander Halavais, associate professor of social technologies at Arizona State University, said, "As there is value in accurate information, the availability of such information will continue to grow. However, when consumers are not directly paying for such accuracy, it will certainly mean a greater degree of misinformation in the public sphere. That means the continuing bifurcation of haves and have-nots, when it comes to trusted news and information."

An **anonymous editor and publisher** commented, "Sadly, many Americans will not pay attention to ANY content from existing or evolving sources. It'll be the continuing dumbing down of the masses, although the 'upper' cadres (educated/thoughtful) will read/see/know, and continue to battle."

An **anonymous respondent** said, "There will be a sort of 'gold standard' set of sources, and there will be the fringe."

Theme 2: The information environment will not improve because technology will create new challenges that can't or won't be countered effectively and at scale

Many who see little hope for improvement of the information environment said technology will not save society from distortions, half-truths, lies and weaponized narratives. An **anonymous business leader** argued, "It is too easy to create fake facts, too labor-intensive to check and too easy to fool checking algorithms." And this response of an anonymous **research scientist based in North America** echoed the view of many participants in this canvassing: "We will develop technologies to help identify false and distorted information, BUT they won't be good enough."

Paul N. Edwards, Perry Fellow in International Security at Stanford University, commented, "Many excellent methods will be developed to improve the information environment, but the history of online systems shows that bad actors can and will always find ways around them."

Vian Bakir, professor in political communication and journalism at Bangor University in Wales, commented, "It won't improve because of 1) the evolving nature of technology – emergent media always catches out those who wish to control it, at least in the initial phase of emergence; 2) online social media and search engine business models favour misinformation spreading; 3) well-resourced propagandists exploit this mix."

Many who expect things will not improve in the next decade said that "white hat" efforts will never keep up with "black hat" advances in information wars. A **user-experience and interaction designer** said, "As existing channels become more regulated, new unregulated channels will continue to emerge."

Subtheme: Those generally acting for themselves and not the public good have the advantage, and they are likely to stay ahead in the information wars

Many of those who expect no improvement of the information environment said those who wish to spread misinformation are highly motivated to use innovative tricks to stay ahead of the methods meant to stop them. They said certain actors in government, business and other individuals with propaganda agendas are highly driven to make technology work in their favor in the spread of misinformation, and there will continue to be more of them.

A number of respondents referred to this as an "arms race." **David Sarokin** of Sarokin Consulting and author of "Missed Information," said, "There will be an arms race between reliable and unreliable information." And **David Conrad**, a chief technology officer, replied, "In the arms race between those who want to falsify information and those who want to produce accurate information, the former will always have an advantage."

Jim Hendler, professor of computing sciences at Rensselaer Polytechnic Institute, commented, "The information environment will continue to change but the pressures of politics, advertising and stock-return-based capitalism rewards those who find ways to manipulate the system, so it will be a constant battle between those aiming for 'objectiveness' and those trying to manipulate the system."

John Markoff, retired journalist and former technology reporter for The New York Times, said, "I am extremely skeptical about improvements related to verification without a solution to the challenge of anonymity on the internet. I also don't believe there will be a solution to the anonymity problem in the near future."

Scott Spangler, principal data scientist at IBM Watson Health, said technologies now exist that make fake information almost impossible to discern and flag, filter or block. He wrote, "Machine learning and sophisticated statistical techniques will be used to accurately simulate real information content and make fake information almost indistinguishable from the real thing."

Jason Hong, associate professor at the School of Computer Science at Carnegie Mellon University, said, "Some fake information will be detectable and blockable, but the vast majority won't. The problem is that it's *still* very hard for computer systems to analyze text, find assertions made in the text and crosscheck them. There's also the issue of subtle nuances or differences of opinion or interpretation. Lastly, the incentives are all wrong. There are a lot of rich and unethical people, politicians, non-state actors and state actors who are strongly incentivized to get fake information out there to serve their selfish purposes."

A **research professor of robotics at Carnegie Mellon University** observed, "Defensive innovation is always behind offensive innovation. Those wanting to spread misinformation will always be able to find ways to circumvent whatever controls are put in place."

A **research scientist for the Computer Science and Artificial Intelligence Laboratory at MIT** said, "Problems will get worse faster than solutions can address, but that only means solutions are more needed than ever."

Subtheme: Weaponized narratives and other false content will be magnified by social media, online filter bubbles and AI

Some respondents expect a dramatic rise in the manipulation of the information environment by nation-states, by individual political actors and by groups wishing to spread propaganda. Their purpose is to raise fears that serve their agendas, create or deepen silos and echo chambers, divide people and set them upon each other, and paralyze or confuse public understanding of the political, social and economic landscape.

This has been referred to as the weaponization of public narratives. Social media platforms such as Facebook, Reddit and Twitter appear to be prime battlegrounds. Bots are often employed, and AI is expected to be implemented heavily in the information wars to magnify the speed and impact of messaging.

A **leading internet pioneer who has worked with the FCC, the UN's International Telecommunication Union (ITU), the General Electric Co. (GE) and other major technology organizations** commented, "The 'internet-as-weapon' paradigm has emerged."

Dean Willis, consultant for Softarmor Systems, commented, "Governments and political groups have now discovered the power of targeted misinformation coupled to personalized understanding of the targets. Messages can now be tailored with devastating accuracy. We're doomed to living in targeted information bubbles."

An **anonymous survey participant** noted, "Misinformation will play a major role in conflicts between nations and within competing parties within nation states."

danah boyd, principal researcher at Microsoft Research and founder of Data & Society, wrote, "What's at stake right now around information is epistemological in nature. Furthermore, information is a source of power and thus a source of contemporary warfare."

Peter Lunenfeld, a professor at UCLA, commented, "For the foreseeable future, the economics of networks and the networks of economics are going to privilege the dissemination of unvetted, unverified and often weaponized information. Where there is a capitalistic incentive to provide content to consumers, and those networks of distribution originate in a huge variety of transnational and even extra-national economies and political systems, the ability to 'control' veracity will be far outstripped by the capability and willingness to supply any kind of content to any kind of user."

These experts noted that the public has turned to social media – especially Facebook – to get its "news." They said the public's craving for quick reads and tabloid-style sensationalism is what makes social media the field of choice for manipulative narratives, which are often packaged to appear like news headlines. They note that the public's move away from more-traditional mainstream news outlets, which had some ethical standards, to consumption of social newsfeeds has weakened mainstream media organizations, making them lower-budget operations that have been forced to compete for attention by offering up clickbait headlines of their own.

An **emeritus professor of communication for a U.S. Ivy League university** noted, "We have lost an important social function in the press. It is being replaced by social media, where there are few if any moral or ethical guidelines or constraints on the performance of informational roles."

A **project leader for a science institute** commented, "We live in an era where most people get their 'news' via social media and it is very easy to spread fake news. The existence of clickbait sites make it easy for conspiracy theories to be rapidly spread by people who do not bother to read entire articles, nor look for trusted sources. Given that there is freedom of speech, I wonder how the situation can ever improve. Most users just read the headline, comment and share without digesting the entire article or thinking critically about its content (if they read it at all)."

Subtheme: The most-effective tech solutions to misinformation will endanger people's dwindling privacy options, and they are likely to limit free speech and remove the ability for people to be anonymous online

The rise of new and highly varied voices with differing agendas and motivations might generally be considered to be a good thing. But some of these experts said the recent major successes by misinformation manipulators have created a threatening environment in which many in the public are encouraging platform providers and governments to expand surveillance. Among the technological solutions for "cleaning up" the information environment are those that work to clearly identify entities operating online and employ algorithms to detect misinformation. Some of these experts expect that such systems will act to identify perceived misbehaviors and label, block, filter or remove some online content and even ban some posters from further posting.

An **educator** commented, "Creating 'a reliable, trusted, unhackable verification system' would produce a system for filtering and hence *structuring* of content. This will end up being a censored information reality."

An **eLearning specialist** observed, "Any system deeming itself to have the ability to 'judge' information as valid or invalid is inherently biased." And a **professor and researcher** noted, "In an open society, there is no prior determination of what information is genuine or fake."

In fact, a share of the respondents predicted that the online information environment will not improve in the next decade because any requirement for authenticated identities would take away the public's highly valued free-speech rights and allow major powers to control the information environment.

A **distinguished professor emeritus of political science at a U.S. university** wrote, "Misinformation will continue to thrive because of the long (and valuable) tradition of

freedom of expression. Censorship will be rejected." An **anonymous respondent** wrote, "There is always a fight between 'truth' and free speech. But because the internet cannot be regulated free speech will continue to dominate, meaning the information environment will not improve."

But another share of respondents said that is precisely why authenticated identities – which are already operating in some places, including China – *will* become a larger part of information systems. A **professor at a major U.S. university** replied, "Surveillance technologies and financial incentives will generate greater surveillance." A **retired university professor** predicted, "Increased censorship and mass surveillance will tend to create official 'truths' in various parts of the world. In the United States, corporate filtering of information will impose the views of the economic elite."

The **executive director of a major global privacy advocacy organization** argued removing civil liberties in order to stop misinformation will not be effective, saying, "'Problematic' actors will be able to game the devised systems while others will be over-regulated."

Several other respondents also cited this as a major flaw of this potential remedy. They argued against it for several reasons, including the fact that it enables even broader government and corporate surveillance and control over more of the public.

Emmanuel Edet, head of legal services at the National Information Technology Development Agency of Nigeria, observed, "The information environment will improve but at a cost to privacy."

Bill Woodcock, executive director of the Packet Clearing House, wrote, "There's a fundamental conflict between anonymity and control of public speech, and the countries that don't value anonymous speech domestically are still free to weaponize it internationally, whereas the countries that do value anonymous speech must make it available to all, [or] else fail to uphold their own principle."

James LaRue, director of the Office for Intellectual Freedom of the American Library Association, commented, "Information systems incentivize getting attention. Lying is a powerful way to do that. To stop that requires high surveillance – which means government oversight which has its own incentives not to tell the truth."

Tom Valovic, contributor to The Technoskeptic magazine and author of "Digital Mythologies," said encouraging platforms to exercise algorithmic controls is not optimal. He wrote: "Artificial intelligence that will supplant human judgment is being pursued aggressively by entities in the Silicon Valley and elsewhere. Algorithmic solutions to replacing human judgment are subject to hidden bias and will ultimately fail to accomplish this goal. They will only continue the centralization of power in a small number of companies that control the flow of information."

Theme 3: The information environment will improve because technology will help label, filter or ban misinformation and thus upgrade the public's ability to judge the quality and veracity of content

Most of the respondents who gave hopeful answers about the future of truth online said they believe technology will be implemented to improve the information environment. They noted their faith was grounded in history, arguing that humans have always found ways to innovate to overcome problems. Most of these experts do not expect there will be a perfect system – but they expect advances. A number said information platform corporations such as Google and Facebook will begin to efficiently police the environment to embed moral and ethical thinking in the structure of their platforms. They hope this will simultaneously enable the screening of content while still protecting rights such as free speech.

Larry Diamond, senior fellow at the Hoover Institution and the Freeman Spogli Institute (FSI) at Stanford University, said, "I am hopeful that the principal digital information platforms will take creative initiatives to privilege more authoritative and credible sources and to call out and demote information sources that appear to be propaganda and manipulation engines, whether human or robotic. In fact, the companies are already beginning to take steps in this direction."

An **associate professor at a U.S. university** wrote, "I do not see us giving up on seeking truth." And a **researcher** based in Europe said, "Technologies will appear that solve the trust issues and reward logic."

Adam Lella, senior analyst for marketing insights at comScore Inc., replied, "There have been numerous other industry-related issues in the past (e.g., viewability, invalid traffic detection, cross-platform measurement) that were seemingly impossible to solve, and yet major progress was made in the past few years. If there is a great amount of pressure from the industry to solve this problem (which there is), then methodologies will be developed and

progress will be made to help mitigate this issue in the long run. In other words, if there's a will, there's way."

Subtheme: Likely tech-based solutions include adjustments to algorithmic filters, browsers, apps and plug-ins and the implementation of 'trust ratings'

Many respondents who hope for improvement in the information environment mentioned ways in which new technological solutions might be implemented.

Bart Knijnenburg, researcher on decision-making and recommender systems and assistant professor of computer science at Clemson University, said, "Two developments will help improve the information environment: 1) News will move to a subscription model (like music, movies, etc.) and subscription providers will have a vested interest in culling down false narratives; 2) Algorithms that filter news will learn to discern the quality of a news item and not just tailor to 'virality' or political leaning."

Laurel Felt, lecturer at the University of Southern California, "There will be mechanisms for flagging suspicious content and providers and then apps and plugins for people to see the 'trust rating' for a piece of content, an outlet or even an IP address. Perhaps people can even install filters so that, when they're doing searches, hits that don't meet a certain trust threshold will not appear on the list."

A **longtime U.S. government researcher and administrator in communications and technology sciences** said, "The intelligence, defense and related U.S. agencies are very actively working on this problem and results are promising."

Amber Case, research fellow at Harvard University's Berkman Klein Center for Internet & Society, suggested withholding ad revenue until veracity has been established. She wrote, "Right now, there is an incentive to spread fake news. It is profitable to do so, profit made by creating an article that causes enough outrage that advertising money will follow. … In order to reduce the spread of fake news, we must deincentivize it financially. If an article bursts into collective consciousness and is later proven to be fake, the sites that control or host that content could refuse to distribute advertising revenue to the entity that created or published it. This would require a system of delayed advertising revenue distribution where ad funds are held until the article is proven as accurate or not. A lot of fake news is created by a few people, and removing their incentive could stop much of the news postings."

Andrea Matwyshyn, a professor of law at Northeastern University who researches innovation and law, particularly information security, observed, "Software liability law will finally begin to evolve. Market makers will increasingly incorporate security quality as a factor relevant to corporate valuation. The legal climate for security research will continue to improve, as its connection to national security becomes increasingly obvious. These changes will drive significant corporate and public sector improvements in security during the next decade."

Larry Keeley, founder of innovation consultancy Doblin, predicted technology will be improved but people will remain the same, writing, "Capabilities adapted from both bibliometric analytics and good auditing practices will make this a solvable problem. However, non-certified, compelling-but-untrue information will also proliferate. So the new divide will be between the people who want their information to be real vs. those who simply want it to *feel* important. Remember that quote from Roger Ailes: 'People don't want to BE informed, they want to FEEL informed.' Sigh."

Anonymous survey participants also responded:
- "Filters and algorithms will improve to both verify raw data, separate 'overlays' and to correct for a feedback loop."
- "Semantic technologies will be able to cross-verify statements, much like meta-analysis."
- "The credibility history of each individual will be used to filter incoming information."
- "The veracity of information will be linked to how much the source is perceived as trustworthy – we may, for instance, develop a trust index and trust will become more easily verified using artificial-intelligence-driven technologies."
- "The work being done on things like verifiable identity and information sharing through loose federation will improve things somewhat (but not completely). That is to say, things will become better but not necessarily good."
- "AI, blockchain, crowdsourcing and other technologies will further enhance our ability to filter and qualify the veracity of information."
- "There will be new visual cues developed to help news consumers distinguish between trusted news sources and others."

Subtheme: Regulatory remedies could include software liability law, required identities, unbundling of social networks like Facebook

A number of respondents believe there will be policy remedies that move beyond whatever technical innovations emerge in the next decade. They offered a range of suggestions, from

regulatory reforms applied to the platforms that aid misinformation merchants to legal penalties applied to wrongdoers. Some think the threat of regulatory reform via government agencies may force the issue of required identities and the abolition of anonymity protections for platform users.

Sonia Livingstone, professor of social psychology at the London School of Economics and Political Science, replied, "The 'wild west' state of the internet will not be permitted to continue by those with power, as we are already seeing with increased national pressure on providers/companies by a range of means from law and regulation to moral and consumer pressures."

Willie Currie, a longtime expert in global communications diffusion, wrote, "The apparent success of fake news on platforms like Facebook will have to be dealt with on a regulatory basis as it is clear that technically minded people will only look for technical fixes and may have incentives not to look very hard, so self-regulation is unlikely to succeed. The excuse that the scale of posts on social media platforms makes human intervention impossible will not be a defense. Regulatory options may include unbundling social networks like Facebook into smaller entities. Legal options include reversing the notion that providers of content services over the internet are mere conduits without responsibility for the content. These regulatory and legal options may not be politically possible to affect within the U.S., but they are certainly possible in Europe and elsewhere, especially if fake news is shown to have an impact on European elections."

Sally Wentworth, vice president of global policy development at the Internet Society, warned against too much dependence upon information platform providers in shaping solutions to improve the information environment. She wrote: "It's encouraging to see some of the big platforms beginning to deploy internet solutions to some of the issues around online extremism, violence and fake news. And yet, it feels like as a society, we are outsourcing this function to private entities that exist, ultimately, to make a profit and not necessarily for a social good. How much power are we turning over to them to govern our social discourse? Do we know where that might eventually lead? On the one hand, it's good that the big players are finally stepping up and taking responsibility. But governments, users and society are being too quick to turn all of the responsibility over to internet platforms. Who holds them accountable for the decisions they make on behalf of all of us? Do we even know what those decisions are?"

A **professor and chair in a department of educational theory, policy and administration** commented, "Some of this work can be done in private markets. Being

banned from social media is one obvious one. In terms of criminal law, I think the important thing is to have penalties/regulations be domain-specific. Speech can be regulated in certain venues, but obviously not in all. Federal (and perhaps even international) guidelines would be useful. Without a framework for regulation, I can't imagine penalties."

Theme 4: The information environment will improve because people will adjust and make things better

Many of those who expect the information environment to improve anticipate that information literacy training and other forms of assistance will help people become more sophisticated consumers. They expect that users will gravitate toward more reliable information – and that knowledge providers will respond in kind.

Frank Kaufmann, founder and director of several international projects for peace activism and media and information, commented, "The quality of news will improve, because things always improve." And **Barry Wellman**, virtual communities expert and co-director of the NetLab Network, said, "Software and people are becoming more sophisticated."

One hopeful respondent said a change in economic incentives can bring about desired change. **Tom Wolzien**, chairman of The Video Call Center and Wolzien LLC, said, "The market will not clean up the bad material, but will shift focus and economic rewards toward the reliable. Information consumers, fed up with false narratives, will increasingly shift toward more-trusted sources, resulting in revenue flowing toward those more trusted sources and away from the junk. This does not mean that all people will subscribe to either scientific or journalistic method (or both), but they will gravitate toward material the sources and institutions they find trustworthy, and those institutions will, themselves, demand methods of verification beyond those they use today."

A **retired public official and internet pioneer** predicted, "1) Education for veracity will become an indispensable element of secondary school. 2) Information providers will become legally responsible for their content. 3) A few trusted sources will continue to dominate the internet."

Irene Wu, adjunct professor of communications, culture and technology at Georgetown University, said, "Information will improve because people will learn better how to deal with masses of digital information. Right now, many people naively believe what they read on social media. When the television became popular, people also believed everything on TV

was true. It's how people choose to react and access to information and news that's important, not the mechanisms that distribute them."

Charlie Firestone, executive director at the Aspen Institute Communications and Society Program, commented, "In the future, tagging, labeling, peer recommendations, new literacies (media, digital) and similar methods will enable people to sift through information better to find and rely on factual information. In addition, there will be a reaction to the prevalence of false information so that people are more willing to act to assure their information will be accurate."

Howard Rheingold, pioneer researcher of virtual communities, longtime professor and author of "Net Smart: How to Thrive Online," noted, "As I wrote in 'Net Smart' in 2012, some combination of education, algorithmic and social systems can help improve the signal-to-noise ratio online – with the caveat that misinformation/disinformation versus verified information is likely to be a continuing arms race. In 2012, Facebook, Google and others had no incentive to pay attention to the problem. After the 2016 election, the issue of fake information has been spotlighted."

Subtheme: Misinformation has always been with us and people have found ways to lessen its impact. The problems will become more manageable as people become more adept at sorting through material

Many respondents agree that misinformation will persist as the online realm expands and more people are connected in more ways. Still, the more hopeful among these experts argue that progress is inevitable as people and organizations find coping mechanisms. They say history validates this. Furthermore, they said technologists will play an important role in helping filter out misinformation and modeling new digital literacy practices for users.

Mark Bunting, visiting academic at Oxford Internet Institute, a senior digital strategy and public policy advisor with 16 years of experience at the BBC and as a digital consultant, wrote, "Our information environment has been immeasurably improved by the democratisation of the means of publication since the creation of the web nearly 25 years ago. We are now seeing the downsides of that transformation, with bad actors manipulating the new freedoms for antisocial purposes, but techniques for managing and mitigating those harms will improve, creating potential for freer, but well-governed, information environments in the 2020s."

Jonathan Grudin, principal design researcher at Microsoft, said, "We were in this position before, when printing presses broke the existing system of information management. A new system emerged and I believe we have the motivation and capability to do it again. It will again involve information channeling more than misinformation suppression; contradictory claims have always existed in print, but have been manageable and often healthy."

Judith Donath, fellow at Harvard University's Berkman Klein Center for Internet & Society and founder of the Sociable Media Group at the MIT Media Lab, wrote, "'Fake news' is not new. The Weekly World News had a circulation of over a million for its mostly fictional news stories that are printed and sold in a format closely resembling a newspaper. Many readers recognized it as entertainment, but not all. More subtly, its presence on the newsstand reminded everyone that anything can be printed."

Joshua Hatch, president of the Online News Association, noted, "I'm slightly optimistic because there are more people who care about doing the right thing than there are people who are trying to ruin the system. Things will improve because people – individually and collectively – will make it so."

Many of these respondents said the leaders and engineers of the major information platform companies will play a significant role. Some said they expect some other systematic and social changes will alter things.

John Wilbanks, chief commons officer at Sage Bionetworks, replied, "I'm an optimist, so take this with a grain of salt, but I think as people born into the internet age move into positions of authority they'll be better able to distill and discern fake news than those of us who remember an age of trusted gatekeepers. They'll be part of the immune system. It's not that the environment will get better, it's that those younger will be better fitted to survive it."

Danny Rogers, founder and CEO of Terbium Labs, replied, "Things always improve. Not monotonically, and not without effort, but fundamentally, I still believe that the efforts to improve the information environment will ultimately outweigh efforts to devolve it."

Bryan Alexander, futurist and president of Bryan Alexander Consulting, replied, "Growing digital literacy and the use of automated systems will tip the balance towards a better information environment."

A number of these respondents said information platform corporations such as Google and Facebook will begin to efficiently police the environment through various technological

enhancements. They expressed faith in the inventiveness of these organizations and suggested the people of these companies will implement technology to embed moral and ethical thinking in the structure and business practices of their platforms, enabling the screening of content while still protecting rights such as free speech.

Patrick Lambe, principal consultant at Straits Knowledge, commented, "All largescale human systems are adaptive. When faced with novel predatory phenomena, counter-forces emerge to balance or defeat them. We are at the beginning of a largescale negative impact from the undermining of a social sense of reliable fact. Counter-forces are already emerging. The presence of largescale 'landlords' controlling significant sections of the ecosystem (e.g., Google, Facebook) aids in this counter-response."

A **professor in technology law at a West Coast-based U.S. university** said, "Intermediaries such as Facebook and Google will develop more-robust systems to reward legitimate producers and punish purveyors of fake news."

A **longtime director for Google** commented, "Companies like Google and Facebook are investing heavily in coming up with usable solutions. Like email spam, this problem can never entirely be eliminated, but it can be managed."

Sandro Hawke, technical staff at the World Wide Web Consortium, predicted, "Things are going to get worse before they get better, but humans have the basic tools to solve this problem, so chances are good that we will. The biggest risk, as with many things, is that narrow self-interest stops people from effectively collaborating."

Anonymous respondents shared these remarks:
- "Accurate facts are essential, particularly within a democracy, so this will be a high, shared value worthy of investment and government support, as well as private-sector initiatives."
- "We are only at the beginning of drastic technological and societal changes. We will learn and develop strategies to deal with problems like fake news."
- "There is a long record of innovation taking place to solve problems. Yes, sometimes innovation leads to abuses, but further innovation tends to solve those problems."
- Consumers have risen up in the past to block the bullshit, fake ads, fake investment scams, etc., and they will again with regard to fake news.
- "As we understand more about digital misinformation we will design better tools, policies and opportunities for collective action."

- ▪ "Now that it is on the agenda, smart researchers and technologists will develop solutions."
- ▪ "The increased awareness of the issue will lead to/force new solutions and regulation that will improve the situation in the long-term even if there are bound to be missteps such as flawed regulation and solutions along the way."

Subtheme: Crowdsourcing will work to highlight verified facts and block those who propagate lies and propaganda. Some also have hopes for distributed ledgers (blockchain)

A number of these experts said solutions such as tagging, flagging or other labeling of questionable content will continue to expand and be of further use in the future in tackling the propagation of misinformation.

J. Nathan Matias, a postdoctoral researcher at Princeton University and previously a visiting scholar at MIT's Center for Civic Media, wrote, "Through ethnography and largescale social experiments, I have been encouraged to see volunteer communities with tens of millions of people work together to successfully manage the risks from inaccurate news."

A **researcher of online harassment working for a major internet information platform** commented, "If there are nonprofits keeping technology in line, such as an ACLU-esque initiative, to monitor misinformation and then partner with spaces like Facebook to deal with this kind of news spam, then yes, the information environment will improve. We also need to move away from clickbaity-like articles, and not algorithmically rely on popularity but on information."

An **engineer based in North America** replied, "The future will attach credibility to the source of any information. The more a given source is attributed to 'fake news,' the lower it will sit in the credibility tree."

Micah Altman, director of research for the Program on Information Science at MIT, commented, "Technological advances are creating forces pulling in two directions: It is increasingly easy to create real-looking fake information; and it is increasingly easy to crowdsource the collection and verification of information. In the longer term, I'm optimistic that the second force will dominate – as transaction cost-reduction appears to be relatively in favor of crowds versus concentrated institutions."

A **past chairman of a major U.S. scientific think tank and former CEO** replied, "[The information environment] should improve because there are many techniques that can be brought to bear both human-mediated – such as collective intelligence via user voting and rating – and technological responses that are either very early in their evolution or not or not deployed at all. See spam as an analog."

Some predicted that digital distributed ledger technologies, known as blockchain, may provide some answers. A longtime **technology editor and columnist based in Europe**, commented, "The blockchain approach used for Bitcoin, etc., could be used to distribute content. DECENT is an early example." And an **anonymous respondent from Harvard University's Berkman Klein Center for Internet & Society** said, "They will be cryptographically verified, with concepts."

But others were less confident that blockchain will work. A **leading researcher studying the spread of misinformation** observed, "I know systems like blockchain are a start, but in some ways analog systems (e.g., scanned voting ballots) can be more resilient to outside influence than digital solutions such as increased encryption. There are always potential compromises when our communication networks are based on human-coded technology and hardware; this [is] less the case with analog-first, digital-second systems."

A **professor of media and communication based in Europe** said, "Right now, reliable and trusted verification systems are not yet available; they may become technically available in the future but the arms race between corporations and hackers is never ending. Blockchain technology may be an option, but every technological system needs to be built on trust, and as long as there is no globally governed trust system that is open and transparent, there will be no reliable verification systems."

Theme 5: Tech can't win the battle. The public must fund and support the production of objective, accurate information. It must also elevate information literacy to be a primary goal of education

There was common agreement among many respondents – whether they said they expect to see improvements in the information environment in the next decade or not – that the problem of misinformation requires significant attention. A share of these respondents urged action in two areas: A bolstering of the public-serving press and an expansive, comprehensive, ongoing information literacy education effort for people of all ages.

A **sociologist doing research on technology and civic engagement at MIT** said, "Though likely to get worse before it gets better, the 2016-2017 information ecosystem problems represent a watershed moment and call to action for citizens, policymakers, journalists, designers and philanthropists who must work together to address the issues at the heart of misinformation."

Michael Zimmer, associate professor and privacy and information ethics scholar at the University of Wisconsin, Milwaukee commented, "This is a social problem that cannot be solved via technology."

Subtheme: Funding and support must be directed to the restoration of a well-fortified, ethical and trusted public press

Many respondents noted that while the digital age has amplified countless information sources it has hurt the reach and influence of the traditional news organizations. These are the bedrock institutions much of the public has relied upon for objective, verified, reliable information – information undergirded by ethical standards and a general goal of serving the common good. These respondents said the information environment cannot be improved without more, well-staffed, financially stable, independent news organizations. They believe that material can rise above misinformation and create a base of "common knowledge" the public can share and act on.

Susan Hares, a pioneer with the National Science Foundation Network (NSFNET) and longtime internet engineering strategist, now a consultant, said, "Society simply needs to decide that the 'press' no longer provides unbiased information, and it must pay for unbiased and verified information."

Christopher Jencks, a professor emeritus at Harvard University, said, "Reducing 'fake news' requires a profession whose members share a commitment to getting it right. That, in turn, requires a source of money to pay such professional journalists. Advertising used to provide newspapers with money to pay such people. That money is drying up, and it seems unlikely to be replaced within the next decade."

Rich Ling, professor of media technology at the School of Communication and Information at Nanyang Technological University, said, "We have seen the consequences of fake news in the U.S. presidential election and Brexit. This is a wake-up call to the news industry, policy makers and journalists to refine the system of news production."

Maja Vujovic, senior copywriter for the Comtrade Group, predicted, "The information environment will be increasingly perceived as a public good, making its reliability a universal need. Technological advancements and civil-awareness efforts will yield varied ways to continuously purge misinformation from it, to keep it reasonably reliable."

An **author and journalist based in North America** said, "I believe this era could spawn a new one – a flight to quality in which time-starved citizens place high value on verified news sources."

A **professor of law at a major U.S. state university** commented, "Things won't get better until we realize that accurate news and information are a public good that require not-for-profit leadership and public subsidy."

Marc Rotenberg, president of the Electronic Privacy Information Center, wrote, "The problem with online news is structural: There are too few gatekeepers, and the internet business model does not sustain quality journalism. The reason is simply that advertising revenue has been untethered from news production."

With precarious funding and shrinking audiences, healthy journalism that serves the common good is losing its voice. **Siva Vaidhyanathan**, professor of media studies and director of the Center for Media and Citizenship at the University of Virginia, wrote, "There are no technological solutions that correct for the dominance of Facebook and Google in our lives. These incumbents are locked into monopoly power over our information ecosystem and as they drain advertising money from all other low-cost commercial media they impoverish the public sphere."

Subtheme: Elevate information literacy; it must become a primary goal at all levels of education

Many of these experts said the flaws in human nature and still-undeveloped norms in the digital age are the key problems that make users susceptible to false, misleading and manipulative online narratives. One potential remedy these respondents suggested is a massive compulsory crusade to educate all in digital-age information literacy. Such an effort, some said, might prepare more people to be wise in what they view/read/believe and possibly even serve to upgrade the overall social norms of information sharing.

Karen Mossberger, professor and director of the School of Public Affairs at Arizona State University, wrote, "The spread of fake news is not merely a problem of bots, but part of a

larger problem of whether or not people exercise critical thinking and information-literacy skills. Perhaps the surge of fake news in the recent past will serve as a wake-up call to address these aspects of online skills in the media and to address these as fundamental educational competencies in our education system. Online information more generally has an almost limitless diversity of sources, with varied credibility. Technology is driving this issue, but the fix isn't a technical one alone."

Mike DeVito, graduate researcher at Northwestern University, wrote, "These are not technical problems; they are human problems that technology has simply helped scale, yet we keep attempting purely technological solutions. We can't machine-learn our way out of this disaster, which is actually a perfect storm of poor civics knowledge and poor information literacy."

Miguel Alcaine, International Telecommunication Union area representative for Central America, commented, "The boundaries between online and offline will continue to blur. We understand online and offline are different modalities of real life. There is and will be a market (public and private providers) for trusted information. There is and will be space for misinformation. The most important action societies can take to protect people is education, information and training."

An **early internet developer and security consultant** commented, "Fake news is not a product of a flaw in the communications channel and cannot be fixed by a fix to the channel. It is due to a flaw in the human consumers of information and can be repaired only by education of those consumers."

An **anonymous respondent from the Harvard University's Berkman Klein Center for Internet & Society** noted, "False information – intentionally or inadvertently so – is neither new nor the result of new technologies. It may now be easier to spread to more people more quickly, but the responsibility for sifting facts from fiction has always sat with the person receiving that information and always will."

An **internet pioneer and rights activist based in the Asia/Pacific region** said, "We as a society are not investing enough in education worldwide. The environment will only improve if both sides of the communication channel are responsible. The reader and the producer of content, both have responsibilities."

Deirdre Williams, retired internet activist, replied, "Human beings are losing their capability to question and to refuse. Young people are growing into a world where those skills are not being taught."

Julia Koller, a learning solutions lead developer, replied, "Information is only as reliable as the people who are receiving it. If readers do not change or improve their ability to seek out and identify reliable information sources, the information environment will not improve."

Ella Taylor-Smith, senior research fellow at the School of Computing at Edinburgh Napier University, noted, "As more people become more educated, especially as digital literacy becomes a popular and respected skill, people will favour (and even produce) better quality information."

Constance Kampf, a researcher in computer science and mathematics, said, "The answer depends on socio-technical design – these trends of misinformation versus verifiable information were already present before the internet, and they are currently being amplified. The state and trends in education and place of critical thinking in curricula across the world will be the place to look to see whether or not the information environment will improve – cyberliteracy relies on basic information literacy, social literacy and technological literacy. For the environment to improve, we need substantial improvements in education systems across the world in relation to critical thinking, social literacy, information literacy, and cyberliteracy (see Laura Gurak's book 'Cyberliteracy')."

Su Sonia Herring, an editor and translator, commented, "Misinformation and fake news will exist as long as humans do; they have existed ever since language was invented. Relying on algorithms and automated measures will result in various unwanted consequences. Unless we equip people with media literacy and critical-thinking skills, the spread of misinformation will prevail."

Responses from additional key experts regarding the future of the information environment

This section features responses by several of the top analysts who participated in this canvassing. Following this wide-ranging set of comments is a much more expansive set of quotations directly tied to the five primary themes identified in this report.

Ignorance breeds frustration and 'a growing fraction of the population has neither the skills nor the native intelligence to master growing complexity'

Mike Roberts, pioneer leader at ICANN and Internet Hall of Fame member, replied, "There are complex forces working both to improve the quality of information on the net, and to corrupt it. I believe the outrage resulting from recent events will, on balance, lead to a net improvement, but viewed with hindsight, the improvement may be viewed as inadequate. The other side of the complexity coin is ignorance. The average man or woman in America today has less knowledge of the underpinnings of his or her daily life than they did 50 or a hundred years ago. There has been a tremendous insertion of complex systems into many aspects of how we live in the decades since World War II, fueled by a tremendous growth in knowledge in general. Even among highly intelligent people, there is a significant growth in personal specialization in order to trim the boundaries of expected expertise to manageable levels. Among educated people, we have learned mechanisms for coping with complexity. We use what we know of statistics and probability to compartment uncertainty. We adopt 'most likely' scenarios for events of which we do not have detailed knowledge, and so on. A growing fraction of the population has neither the skills nor the native intelligence to master growing complexity, and in a competitive social environment, obligations to help our fellow humans go unmet.

"Educated or not, no one wants to be a dummy — all the wrong connotations. So ignorance breeds frustration, which breeds acting out, which breeds antisocial and pathological behavior, such as the disinformation, which was the subject of the survey, and many other undesirable second order effects. Issues of trustable information are certainly important, especially since the technological intelligentsia command a number of tools to combat untrustable info. But the underlying pathology won't be tamed through technology alone. We need to replace ignorance and frustration with better life opportunities that restore confidence — a tall order and a tough agenda. Is there an immediate nexus between widespread ignorance and corrupted information sources? Yes, of course. In fact, there is a virtuous circle where acquisition of trustable information reduces ignorance, which leads to better use of better information, etc."

The truth of news is murky and multifaceted

Judith Donath, fellow at Harvard University's Berkman Klein Center for Internet & Society and founder of the Sociable Media Group at the MIT Media Lab, wrote, "Yes, trusted methods will emerge to block false narratives and allow accurate information to prevail, and, yes, the quality and veracity of information online will deteriorate due to the spread of unreliable, sometimes even dangerous, socially destabilizing ideas. Of course, the definition of 'true' is sometimes murky. Experimental scientists have many careful protocols in place to assure the veracity of their work, and the questions they ask have well-defined answers – and still there can be controversy about what is true, what work was free from outside influence. The truth of news stories is far murkier and multi-faceted. A story can be distorted, disproportional, meant to mislead – and still, strictly speaking, factually accurate. … But a pernicious harm of fake news is the doubt it sows about the reliability of all news. Donald Trump's repeated 'fake news' smears of The New York Times, Washington Post, etc., are among his most destructive non-truths."

'Algorithms weaponize rhetoric,' influencing on a mass scale

Susan Etlinger, industry analyst at Altimeter Research, said, "There are two main dynamics at play: One is the increasing sophistication and availability of machine learning algorithms and the other is human nature. We've known since the ancient Greeks and Romans that people are easily persuaded by rhetoric; that hasn't changed much in two thousand years. Algorithms weaponize rhetoric, making it easier and faster to influence people on a mass scale. There are many people working on ways to protect the integrity and reliability of information, just as there are cybersecurity experts who are in a constant arms race with cybercriminals, but to put as much emphasis on 'information' (a public good) as 'data' (a personal asset) will require a pretty big cultural shift. I suspect this will play out differently in different parts of the world."

There's no technical solution for the fact that 'news' is a social bargain

Clay Shirky, vice provost for educational technology at New York University, replied, "'News' is not a stable category – it is a social bargain. There's no technical solution for designing a system that prevents people from asserting that Obama is a Muslim but allows them to assert that Jesus loves you."

'Strong economic forces are incentivizing the creation and spread of fake news'

Amy Webb, author and founder of the Future Today Institute, wrote, "In an era of social, democratized media, we've adopted a strange attitude. We're simultaneously skeptics and

true believers. If a news story reaffirms what we already believe, it's credible – but if it rails against our beliefs, it's fake. We apply that same logic to experts and sources quoted in stories. With our limbic systems continuously engaged, we're more likely to pay attention to stories that make us want to fight, take flight or fill our social media accounts with links. As a result, there are strong economic forces incentivizing the creation and spread of fake news. In the digital realm, attention is currency. It's good for democracy to stop the spread of misinformation, but it's bad for business. Unless significant measures are taken in the present – and unless all the companies in our digital information ecosystem use strategic foresight to map out the future – I don't see how fake news could possibly be reduced by 2027."

Propagandists exploit whatever communications channels are available

Ian Peter, internet pioneer, historian and activist, observed, "It is not in the interests of either the media or the internet giants who propagate information, nor of governments, to create a climate in which information cannot be manipulated for political, social or economic gain. Propaganda and the desire to distort truth for political and other ends have always been with us and will adapt to any form of new media which allows open communication and information flows."

Expanding information outlets erode opportunities for a 'common narrative'

Kenneth R. Fleischmann, associate professor at the School of Information at the University of Texas, Austin, wrote, "Over time, the general trend is that a proliferation of information and communications technologies (ICTs) has led to a proliferation of opportunities for different viewpoints and perspectives, which has eroded the degree to which there is a common narrative – indeed, in some ways, this parallels a trend away from monarchy toward more democratic societies that welcome a diversity of perspectives – so I anticipate the range of perspectives to increase, rather than decrease, and for these perspectives to include not only opinions but also facts, which are inherently reductionist and can easily be manipulated to suit the perspective of the author, following the old aphorism about statistics Mark Twain attributed to Benjamin Disraeli ['There are three kinds of lies: lies, damned lies and statistics.'], which originally referred to experts more generally."

'Broken as it might be, the internet is still capable of routing around damage'

Paul Saffo, longtime Silicon-Valley-based technology forecaster, commented, "The information crisis happened in the shadows. Now that the issue is visible as a clear and urgent danger, activists and people who see a business opportunity will begin to focus on it. Broken as it might be, the internet is still capable of routing around damage."

It will be impossible to distinguish between fake and real video, audio, photos

Marina Gorbis, executive director of the Institute for the Future, predicted, "It's not going to be better or worse but very different. Already we are developing technologies that make it impossible to distinguish between fake and real video, fake and real photographs, etc. We will have to evolve new tools for authentication and verification. We will probably have to evolve both new social norms as well as regulatory mechanisms if we want to maintain online environment as a source of information that many people can rely on."

A 'Cambrian explosion' of techniques will arise to monitor the web, non-web sources

Stowe Boyd, futurist, publisher and editor-in-chief of Work Futures, said, "The rapid rise of AI will lead to a Cambrian explosion of techniques to monitor the web and non-web media sources and social networks and rapidly identifying and tagging fake and misleading content."

Well, there's good news and bad news about the information future …

Jeff Jarvis, professor at the City University of New York's Graduate School of Journalism, commented, "Reasons for hope: Much attention is being directed at manipulation and disinformation; the platforms may begin to recognize and favor quality; and we are still at the early stage of negotiating norms and mores around responsible civil conversation. Reasons for pessimism: Imploding trust in institutions; institutions that do not recognize the need to radically change to regain trust; and business models that favor volume over value."

A fear of the imposition of pervasive censorship

Jim Warren, an internet pioneer and open-government/open-records/open-meetings advocate, said, "False and misleading information has always been part of all cultures (gossip, tabloids, etc.). Teaching judgment has always been the solution, and it always will be. I (still) trust the longstanding principle of free speech: The best cure for 'offensive' speech is MORE speech. The only major fear I have is of massive communications conglomerates imposing pervasive censorship."

People have to take responsibility for finding reliable sources

Steven Miller, vice provost for research at Singapore Management University, wrote, "Even now, if one wants to find reliable sources, one has no problem doing that, so we do not lack reliable sources of news today. It is that there are all these other options, and people can choose to live in worlds where they ignore so-called reliable sources, or ignore a multiplicity of sources that can be compared, and focus on what they want to believe. That type of

situation will continue. Five or 10 years from now, I expect there to continue to be many reliable sources of news, and a multiplicity of sources. Those who want to seek out reliable sources will have no problems doing so. Those who want to make sure they are getting a multiplicity of sources to see the range of inputs, and to sort through various types of inputs, will be able to do so, but I also expect that those who want to be in the game of influencing perceptions of reality and changing the perceptions of reality will also have ample means to do so. So the responsibility is with the person who is seeking the news and trying to get information on what is going on. We need more individuals who take responsibility for getting reliable sources."

About this canvassing of experts

The expert predictions reported here about the impact of the internet over the next 10 years came in response to a question asked by Pew Research Center and Elon University's Imagining the Internet Center in an online canvassing conducted between July 2 and Aug. 7, 2017. This is the eighth "Future of the Internet" study the two organizations have conducted together. For this project, we invited more than 8,000 experts and members of the interested public to share their opinions on the likely future of the internet. Overall, 1,116 people responded and answered this question:

> ***The rise of "fake news" and the proliferation of doctored narratives that are spread by humans and bots online are challenging publishers and platforms. Those trying to stop the spread of false information are working to design technical and human systems that can weed it out and minimize the ways in which bots and other schemes spread lies and misinformation.***
>
> ***The question: <ins>In the next 10 years, will trusted methods emerge to block false narratives and allow the most accurate information to prevail in the overall information ecosystem? Or will the quality and veracity of information online deteriorate due to the spread of unreliable, sometimes even dangerous, socially-destabilizing ideas?</ins>***

Respondents were then asked to choose one of the following answers and follow up by answering a series of six questions allowing them to elaborate on their thinking:

> The information environment **will improve** – In the next 10 years, on balance, the information environment will be IMPROVED by changes that reduce the spread of lies and other misinformation online
>
> The information environment **will NOT improve** – In the next 10 years, on balance, the information environment will NOT BE improved by changes designed to reduce the spread of lies and other misinformation online

The web-based instrument was first sent directly to a list of targeted experts identified and accumulated by Pew Research Center and Elon University during the previous seven "Future of the Internet" studies, as well as those identified across 12 years of studying the internet realm during its formative years. Among those invited were people who are active in the global internet policy community and internet research activities, such as the Internet

Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN), Internet Society (ISOC), International Telecommunications Union (ITU), Association of Internet Researchers (AoIR), and Organization for Economic Cooperation and Development (OECD). We also invited a large number of professionals, innovators and policy people from technology businesses; government, including the National Science Foundation, Federal Communications Commission and the European Union; the media and media-watchdog organizations; and think tanks and interest networks (for instance, those that include professionals and academics in anthropology, sociology, psychology, law, political science and communications), as well as globally located people working with communications technologies in government positions; top universities' engineering/computer science departments, business/entrepreneurship faculties, and graduate students and postgraduate researchers; plus many who are active in civil society organizations such as the Association for Progressive Communications (APC), the Electronic Privacy Information Center (EPIC), the Electronic Frontier Foundation (EFF) and Access Now; and those affiliated with newly emerging nonprofits and other research units examining ethics and the digital age. Invitees were encouraged to share the canvassing questionnaire link with others they believed would have an interest in participating, thus there was a "snowball" effect as the invitees were joined by those they invited to weigh in.

Since the data are based on a nonrandom sample, the results are not projectable to any population other than the individuals expressing their points of view in this sample.

The respondents' remarks reflect their personal positions and are not the positions of their employers; the descriptions of their leadership roles help identify their background and the locus of their expertise.

About 74% of respondents identified themselves as being based in North America; the others hail from all corners of the world. When asked about their "primary area of internet interest," 39% identified themselves as research scientists; 7% as entrepreneurs or business leaders; 10% as authors, editors or journalists; 10% as advocates or activist users; 11% as futurists or consultants; 3% as legislators, politicians or lawyers; and 4% as pioneers or originators. An additional 22% specified their primary area of interest as "other."

More than half the expert respondents elected to remain anonymous. Because people's level of expertise is an important element of their participation in the conversation, anonymous respondents were given the opportunity to share a description of their internet expertise or background, and this was noted where relevant in this report.

Here are some of the key respondents in this report (note, position titles and organization names were provided by respondents at the time of this canvassing and may not be current):

Bill Adair, Knight Professor of Journalism and Public Policy at Duke University; **Daniel Alpert**, managing partner at Westwood Capital; **Micah Altman**, director of research for the Program on Information Science at MIT; **Robert Atkinson**, president of the Information Technology and Innovation Foundation; **Patricia Aufderheide**, professor of communications at American University; **Mark Bench**, former executive director of World Press Freedom Committee; **Walter Bender**, senior research scientist with MIT/Sugar Labs; **danah boyd**, founder of Data & Society; **Stowe Boyd**, futurist, publisher and editor-in-chief of Work Futures; **Tim Bray**, senior principal technologist at Amazon; **Marcel Bullinga**, trend watcher and keynote speaker; **Eric Burger**, research professor of computer science and director of the Georgetown Center for Secure Communication; **Jamais Cascio**, distinguished fellow at the Institute for the Future; **Barry Chudakov**, founder and principal at Sertain Research and StreamFuzion Corp.; **David Conrad**, well-known CTO; **Larry Diamond**, senior fellow at the Hoover Institution and the Freeman Spogli Institute (FSI) at Stanford University; **Judith Donath**, Harvard University's Berkman Klein Center for Internet & Society; **Stephen Downes**, researcher at the National Research Council of Canada; **Johanna Drucker**, professor of information studies at the University of California, Los Angeles; **Andrew Dwyer**, expert in cybersecurity and malware at the University of Oxford; **Esther Dyson**, entrepreneur, former journalist and founding chair at ICANN; **Glenn Edens**, CTO for Technology Reserve at PARC, a Xerox company; **Paul N. Edwards**, fellow in international security at Stanford University; **Mohamed Elbashir**, senior manager for internet regulatory policy at Packet Clearing House; **Susan Etlinger**, industry analyst at Altimeter Research; **Bob Frankston,** internet pioneer and software innovator; **Oscar Gandy**, professor emeritus of communication at the University of Pennsylvania; **Mark Glaser**, publisher and founder of MediaShift.org; **Marina Gorbis**, executive director at the Institute for the Future; **Jonathan Grudin**, principal design researcher at Microsoft; **Seth Finkelstein**, consulting programmer and EFF Pioneer Award winner; **Susan Hares**, a pioneer with the NSFNET and longtime internet engineering strategist; **Jim Hendler**, professor of computing sciences at Rensselaer Polytechnic Institute; **Starr Roxanne Hiltz**, author of "Network Nation" and distinguished professor of information systems; **Helen Holder**, distinguished technologist at Hewlett Packard (HP); **Jason Hong**, associate professor at the School of Computer Science at Carnegie Mellon University; **Christian H. Huitema**, past president of the Internet Architecture Board; **Alan Inouye**, director of public policy for the American Library Association; **Larry Irving**, CEO of The Irving Group; **Brooks Jackson** of FactCheck.org; **Jeff Jarvis**, a professor at the City University of New York's Graduate School of Journalism; **Christopher Jencks**, a professor emeritus at Harvard University; **Bart Knijnenburg**, researcher on decision-

making and recommender systems at Clemson University; **James LaRue**, director of the Office for Intellectual Freedom of the American Library Association; **Jon Lebkowsky**, web consultant, developer and activist; **Mark Lemley**, professor of law at Stanford University; **Peter Levine**, professor and associate dean for research at Tisch College of Civic Life; **Mike Liebhold**, senior researcher and distinguished fellow at the Institute for the Future; **Sonia Livingstone**, professor of social psychology at the London School of Economics; **Alexios Mantzarlis**, director of the International Fact-Checking Network; **John Markoff**, retired senior technology writer at The New York Times; **Andrea Matwyshyn**, a professor of law at Northeastern University; **Giacomo Mazzone**, head of institutional relations for the World Broadcasting Union; **Jerry Michalski**, founder at REX; **Riel Miller**, team leader in futures literacy for UNESCO; **Andrew Nachison**, founder at We Media; **Gina Neff**, professor at the Oxford Internet Institute; **Alex 'Sandy' Pentland**, member of the U.S. National Academy of Engineering and the World Economic Forum; **Ian Peter**, internet pioneer, historian and activist; **Justin Reich**, executive director at the MIT Teaching Systems Lab; **Howard Rheingold**, pioneer researcher of virtual communities and author of "Net Smart"; **Mike Roberts**, Internet Hall of Fame member and first president and CEO of ICANN; **Michael Rogers**, author and futurist at Practical Futurist; **Tom Rosenstiel**, director of the American Press Institute; **Marc Rotenberg**, executive director of EPIC; **Paul Saffo**, longtime Silicon-Valley-based technology forecaster; **David Sarokin**, author of "Missed Information: Better Information for Building a Wealthier, More Sustainable Future"; **Henning Schulzrinne**, Internet Hall of Fame member and professor at Columbia University; **Jack Schofield**, longtime technology editor and now columnist at The Guardian; **Clay Shirky**, vice provost for educational technology at New York University; **Ben Shneiderman**, professor of computer science at the University of Maryland; **Ludwig Siegele**, technology editor at The Economist; **Evan Selinger**, professor of philosophy at Rochester Institute of Technology; **Scott Spangler**, principal data scientist at IBM Watson Health; **Brad Templeton**, chair emeritus for the Electronic Frontier Foundation; **Richard D. Titus**, CEO for Andronik; **Joseph Turow**, professor of communication at the University of Pennsylvania; **Stuart A. Umpleby**, professor emeritus at George Washington University; **Siva Vaidhyanathan**, professor of media studies and director of the Center for Media and Citizenship at the University of Virginia; **Tom Valovic**, The Technoskeptic magazine; Hal Varian, chief economist for Google; **Jim Warren**, longtime technology entrepreneur and activist; **Amy Webb**, futurist and CEO at the Future Today Institute; **David Weinberger**, senior researcher at Harvard University's Berkman Klein Center for Internet & Society; **Kevin Werbach**, professor of legal studies and business ethics at the Wharton School at the University of Pennsylvania; **John Wilbanks**, chief commons officer at Sage Bionetworks; and **Irene Wu**, adjunct professor of communications, culture and technology at George Washington University.

A brief selection of institutions at which respondents work or have affiliations:

Adroit Technologies, Altimeter Group, Amazon, American Press Institute, Asia-Pacific Network Information Centre (APNIC), AT&T, BrainPOP, Brown University, BuzzFeed, Carnegie Mellon University, Center for Advanced Communications Policy, Center for Civic Design, Center for Democracy/Development/Rule of Law (CDDRL), Center for Media Literacy, Cesidian Root, Cisco, City University of New York's Graduate School of Journalism, Cloudflare, CNRS, Columbia University, comScore, Comtrade Group, Craigslist, Data & Society, Deloitte, DiploFoundation, Electronic Frontier Foundation, Electronic Privacy Information Center, Farpoint Group, Federal Communications Commission (FCC), Fundación REDES, Future Today Institute, George Washington University, Google, Hackerati, Harvard University's Berkman Klein Center for Internet & Society, Harvard Business School, Hewlett Packard (HP), Hyperloop, IBM Research, IBM Watson Health, ICANN, Ignite Social Media, Institute for the Future, International Fact-Checking Network, Internet Engineering Task Force, Internet Society, International Telecommunication Union (ITU), Karlsruhe Institute of Technology, Kenya Private Sector Alliance, KMP Global, LearnLaunch, LMU Munich, Massachusetts Institute of Technology (MIT), Mathematica Policy Research, MCNC, MediaShift.org, Meme Media, Microsoft, Mimecast, Nanyang Technological University, National Academies of Sciences/Engineering/Medicine, National Research Council of Canada, National Science Foundation, Netapp, NetLab Network, Network Science Group of Indiana University, Neural Archives Foundation, New York Law School, New York University, OpenMedia, Oxford University, Packet Clearing House, Plugged Research, Princeton University, Privacy International, Qlik, Quinnovation, RAND Corporation, Rensselaer Polytechnic Institute, Rochester Institute of Technology, Rose-Hulman Institute of Technology, Sage Bionetworks, Snopes.com, Social Strategy Network, Softarmor Systems, Stanford University, Straits Knowledge, Syracuse University, Tablerock Network, Telecommunities Canada, Terebium Labs, Tetherless Access, UNESCO, U.S. Department of Defense, University of California (Berkeley, Davis, Irvine and Los Angeles campuses), University of Michigan, University of Milan, University of Pennsylvania, University of Toronto, Way to Wellville, We Media, Wikimedia Foundation, Worcester Polytechnic Institute, World Broadcasting Union, W3C, Xerox's PARC, Yale Law.

Complete sets of for-credit and anonymous responses can be found here:

- http://www.elon.edu/e-web/imagining/surveys/2017_survey/future_of_the_information_environment.xhtml
- http://www.elon.edu/e-web/imagining/surveys/2017_survey/future_of_information_environment_anon.xhtml
- http://www.elon.edu/e-web/imagining/surveys/2017_survey/future_of_information_environment_credit.xhtml

Theme 1: The information environment will *not* improve. The problem is human nature

Misinformation and "fake news" have been around for as long as people have communicated. But today's instant, low-budget, far-reaching communications capabilities have the potential to make the problem orders of magnitude more dangerous than in the past.

As [Frederic Filloux explains](): "'Misinformation' – a broader concept that encompasses intentional deception, low-quality information and hyperpartisan news – is seen as a serious threat to democracies. ... The Dark Web harbours vast and inexpensive resources to take advantage of the social loudspeaker. For a few hundred bucks, anyone can buy thousands of social media accounts that are old enough to be credible, or millions of email addresses. Also, by using Mechanical Turk or similar cheap crowdsourcing services widely available on the open web, anyone can hire legions of 'writers' who will help to propagate any message or ideology on a massive scale. That trade is likely to grow and flourish with the emergence of what experts call the 'weaponized artificial intelligence propaganda,' a black magic that leverages microtargeting where fake news stories (or hyperpartisan ones) will be tailored down to the individual level and distributed by a swarm of bots. What we see unfolding right before our eyes is nothing less than Moore's Law applied to the distribution of misinformation: An exponential growth of available technology coupled with a rapid collapse of costs."

Roughly half the experts in this canvassing generally agreed with Filloux's description of how technologies are emerging to enable misinformation distribution, and they worry about what may come next. Many expressed deep concerns about people's primal traits, behaviors and cognitive responses and how they play out in new digital spaces. They said digital platforms are often amplifying divisions and contentiousness, driving users to mistrust those not in their "tribe."

William L. Schrader, a former CEO with PSINet, wrote, "Mankind has always lied, and always will; which is why the winners of wars get to write the history their way and others have no say, but with the internet, the losers have a say! So which is better? Both sides, or just the winner? We have both sides today."

Respondents discussed the scale of the problem and how difficult it can be to assess and weed out bad information, saying that even sophisticated information consumers are likely to struggle in the coming information environment and credulous consumers may have little chance of working their way to true information. **Nathaniel Borenstein**, chief scientist at

Mimecast, commented, "Internet technologies permit anyone to publish anything. Any attempt to improve the veracity of news must be done by some authority, and people don't trust the same authorities, so they will ultimately get the news that their preferred authority wants them to have. There is nothing to stop them choosing an insane person as their authority."

More people = more problems. The internet's continuous growth and accelerating innovation allow more people and artificial intelligence (AI) to create and instantly spread manipulative narratives

Some experts argued that the scale of the problem – too much bad information too easily disseminated – is their major concern. The internet facilitates too many information actors with divergent motives to allow for consistent identification of reliable information and effective strategies to flag false information.

Andrew Odlyzko, professor of math and former head of the University of Minnesota's Supercomputing Institute, observed, "'What is truth has almost always been a contentious issue. Technological developments make it possible for more groups to construct their 'alternate realities,' and the temptation to do it is likely to be irresistible."

Andrew Nachison, author, futurist and founder of WeMedia, noted, "Technology will not overcome malevolence. Systems built to censor communication, even malevolent communication, will be countered by people who circumvent them."

David Weinberger, writer and senior researcher at Harvard University's Berkman Klein Center for Internet & Society, noted, "It is an urgent problem, so it will be addressed urgently, and imperfectly."

Jan Schaffer, executive director of J-Lab, said, "There are so many people seeking to disseminate fake news and produce fake videos in which officials appear to be talking that it will be impossible to shut them all down. Twitter and Facebook and other social media players could play a stronger role. Only a few national news organizations will be trusted sources – if they can manage to survive."

Brian Cute, longtime internet executive and ICANN participant, said, "I am not optimistic that humans will collectively develop the type of rigorous habits that can positively impact the fake news environment. Humans have to become more effective consumers of information for the environment to improve. That means they have to be active and effective

'editors' of the information they consume. And that means they have to be active and effective editors of the information they *share* on the internet, because poorly researched information feeds the fake news cycle."

Rajnesh Singh, Asia-Pacific director for a major internet policy and standards organization, observed, "The issue will be how to cope with the volume of information that is generated and the proportion of it that is inaccurate or fake."

Steve Axler, a user-experience researcher, replied, "Social media and the web are on too large a scale to control content."

A **software engineer** referred to the human quest for power and authority as the underlying problem, writing, "Automation, control and monopolization of information sources and distribution channels will expand, with a goal to monetize or obfuscate."

Allan Shearer, associate professor at the University of Texas, Austin, observed, "The problem is the combination of the proliferation of platforms to post news and an increasing sense of agency in each person that his/her view matter, and the blurring of facts and opinions."

A **vice president for stakeholder engagement** said, "With a deluge of data, people look for shortcuts to determine what they believe, making them susceptible to filter bubbles and manipulation."

Jens Ambsdorf, CEO at The Lighthouse Foundation, based in Germany, replied, "The variability of information will increase. The amount of 'noise' and retweeted stuff will increase and without skills and tools it will become more difficult for citizens to sort out reliable from unreliable sources."

A **professor at Harvard Business School** wrote, "The vast majority of new users and a majority of existing users are not sophisticated readers of news facts, slants or content, nor should we expect them to be. Meanwhile, the methods for manipulation are getting better."

Diana Ascher, information scholar at the University of California, Los Angeles, observed, "Fake news, misinformation, disinformation and propaganda are not new; what's new is the algorithmic propagation of such information. In my research, I call this the new yellow journalism."

Axel Bender, a group leader for Defence Science and Technology (DST) Group of Australia, said, "The veracity of information is unlikely to improve as 1) there will be an increase in the number and heterogeneity of (mis)information sources; and 2) artificially intelligent misinformation detectors will not be smart enough to recognise semantically sophisticated misinformation."

Adrian Schofield, an applied research manager based in Africa, commented, "The passive majority remains blissfully unaware of the potential (and real) threats posed by malicious operators in the ICT [information and communications technology] space. As fast as the good guys develop barriers … the bad guys will devise ways to leapfrog the barriers. It's cheap and it's borderless."

Collette Sosnowy, a respondent who shared no additional personal details, wrote, "The sources of information and the speed with which they are spread are so numerous I don't see how they could effectively be curtailed."

Monica Murero, a professor and researcher based in Europe, wrote, "The information environment will not improve easily, in part because of the technical nature of digitalized information and the tendency of re-elaborating and sharing information by anyone able to act in a prosumeristic fashion. For example, fake news (or unreliable information) is easy to produce thanks to the technical nature of digital information (duplicable, easy to modify, free of costs, durable over time, etc.) and the availability of programs [software] and tools (pre-designed format for elaborating images and contents) are widely available to anyone at an easy reach (a few words on any search engine). In the next 10 years I foresee disparities among countries in terms of improvements and deteriorations of the information environment (depending on country and their regulation, i.e., China, Europe, North Korea, U.S., etc.)."

Sebastian Benthall, junior research scientist, New York University Steinhardt, responded, "The information environment is getting more complex. This complexity provides more opportunities for production and consumption of misinformation."

Tiffany Shlain, Filmmaker & Founder, The Webby Award, wrote, "I am concerned that as artificial intelligences advance, distinguishing between what is written by a human and what is generated by a bot will become more difficult."

Matt Moore, a business leader, observed, "The pressures driving the creation of 'fake news' will only increase – political partisanship, inter-state rivalry, plus the technologies needed to

create and disseminate fake news will also increase in power and decrease in cost. New verification tools will emerge but these will not be sufficient to counter these other forces."

Jon Lebkowsky, web consultant/developer, author and activist, commented, "Given the complexity of the evolving ecosystem, it will be hard to get a handle on it. The decentralization of education is another difficult aspect: universal centralized digital literacy education could potentially mitigate the problem, but we could be moving away from universal standard educational systems."

The **executive director of a major global privacy advocacy organization** said, "What's essentially happening today is basic human behaviour and powerful systems at play. It is only out-of-touch advocates and politicians who believe we can somehow constrain these results."

Veronika Valdova, managing partner at Arete-Zoe, noted, "Rogue regimes like Russia will continue exploiting the information environment to gain as much power and influence as possible. Jurisdictional constraints will make intervention less practicable. Also, whilst the overall information environment in English-speaking countries might improve due to the employment of artificial intelligence and easier neutralization of bots, this may not necessarily be the case for small nations in Europe where the environment is compartmented by language."

Joel Reidenberg, chair and professor of law at Fordham University, wrote, "The complexity of the information ecosystem and the public's preference for filter bubbles will make improvements very difficult to achieve at scale."

Garrett A. Turner, a vice president for global engineering, predicted, "The information environment will not improve because [promotion of misinformation] has proven to be very effective and it is also extremely time-consuming to validate or police. In the transmission of information online it is difficult to decipher factual news from entertainment."

An **author and journalist based in North America** wrote, "Fragmenting social groups and powerful economic interests have the motive and means to create their own narratives. Who is the status quo that can defeat this in a modern society that likes to define itself as disruptive, countercultural, rebel, radical – choose the term that fits your tribe."

Anonymous respondents also commented:

- "There is just too much information and the environment has become so fragmented."
- "The sheer volume of information and communication is too much."
- "Many users seem to be indifferent or confused about objectively accurate information, which is difficult to confirm in an environment of information overload."

Humans are by nature selfish, tribal, gullible convenience seekers who put the most trust in that which seems familiar

A share of these respondents supported a view articulated by **Peter Eckart**, director of information technology at the Illinois Public Health Institute. He argued, "The problem isn't with the sources of information, but with the hearers of it. If we don't increase our collective ability to critically analyze the information before us, all of the expert systems in the world won't help us." People believe what they want to believe, these experts argued, and now have new ways to disseminate the things they believe to others.

David Sarokin, writer, commented, "People spread the information they want to spread, reliable or not. There's no technology that will minimize that tendency."

Helen Holder, distinguished technologist at Hewlett Packard (HP), said, "People have a strong tendency to believe things that align with their existing understanding or views. Unreliable information will have a substantial advantage wherever it reinforces biases, making it difficult to discredit or correct. Also, people are more inclined to believe information received from more than one source, and the internet makes it trivial to artificially simulate multiple sources and higher levels of popular support or belief."

Bill Jones, chairman of Global Village Ltd., predicted, "Trust can be so easily abused that it's our collective ability to discern false from true, which ultimately is the key, but that is fraught with challenges. No one can do it for us.

A **futurist/consultant based in North America** said, "The toxicity of the modern information landscape is as much attributable to vulnerabilities in human neurobiology as it is to anything embedded in software systems. Many of us, including those with the most control over the information environment, badly want things to improve, but it's unclear to me that purely technical methods can solve these problems."

Cliff Cook, planning information manager for the City of Cambridge, Massachusetts, noted, "Fake news and related problems thrive when they have a receptive audience. The underlying problem is not one of fake news – rumors were no doubt a problem in ancient Rome and the court of King Henry VIII – but the presence of a receptive audience. Until a means is found to heal the fundamental breakdown in trust among Americans, I do not see matters improving, no matter what the technical fix."

An **anonymous respondent** wrote, "Google and Facebook are focusing money and attention on the problem of false information. … We have not yet reached a societal tipping point where facts are valued, however."

Matt Armstrong, an independent research fellow working with King's College and former executive director of the U.S. Advisory Commission on Public Diplomacy, replied, "The influence of bad information will not change until people change. At present, there is little indication that people will alter their consumption habits. When 'I heard it on the internet' is a mark of authority rather than derision as it was, we are in trouble. This is coupled with the disappointing reality that we are now in a real war of words where many consumers do not check whether the words are/were/will be supported by actions or facts. The words of now are all that matter to too many audiences."

An **assistant professor of political science** wrote, "Improving information environments does little to address demand for misinformation by users."

An **anonymous research scientist** observed, "False narratives are not new to the internet, but authority figures are now also beginning to create them."

A **former journalism professor and author of a book on the future of news** commented, "The information superhighway's very speed and ease have made people sloppier thinkers, not more discerning."

A **researcher based in Europe** replied, "The problem with fake news is not a technological one, but one related to human nature, fear, ignorance and power. … In addition, as new tools are developed to fight fake news, those interested in spreading them will also become more savvy and sophisticated."

Walter Bender, a senior research scientist at MIT, wrote, "I don't think the problem is technological. It is social, and it is not much different from the American Aurora of 1800 in Philadelphia [a one-sided and largely discredited publication in American Revolution times].

People want to believe what reinforces their current positions, and there will be 'publishers' willing to accommodate them."

Many respondents mentioned distrust in authority as a motivating factor behind the uptick in the spread of misinformation, and some said political polarization and the destruction of trust are feeding the emergence of more misinformation.

Daniel Kreiss, associate professor of communication at University of North Carolina, Chapel Hill, commented, "Misinformation/fake news/ideological/identity media is a political problem. They are the outcome, not the cause, of political polarization."

A **senior fellow at a center focusing on democracy and the rule of law** wrote, "Many people do not care about the veracity of the news they consume and circulate to others, and these people will continue spreading false information; those who do so from within established democracies can be punished/penalized, but many will remain in non-democracies where access to reliable information will deteriorate. My prediction is that in parts of the world things will improve, in others they will deteriorate. On average things will not improve."

Anonymous respondents also wrote:
- "To really solve this issue we need to look deeper at what truth means and who cares about it. It will take more than a decade to sort that out and implement solutions."
- "Collective-action problems require a collective-action response, and I don't think we'll manage that in the international environment."
- "The information environment reflects society at its best or worst; changes in human behavior, not technology, will impact on the information environment."
- "At best, the definition of 'lie' will simply change and official disinformation will be called information anyway."
- "I have yet to see any evidence that the most-active political media consumers want more facts and less opinion."
- "There has never been a wholly truthful human environment, and there are too many vested interests in fantasy, fiction and untruths."
- "I do not think technology can keep up with people's creativity or appetite for information they find congenial to their pre-existing beliefs."
- "As long as people want to believe a lie, the lie will spread."
- "From propaganda to humour, the natural drive to share information will overcome any obstacles that hinder it."

▪   "It will be a constant game of whack-a-mole, and polarization has now come to facts. It's almost like facts are a philosophy class exercise now – what is truth?"

In existing economic, political and social systems, the powerful corporate and government leaders most able to improve the information environment profit most when it is in turmoil

A number of these experts predicted that little will change as long as social media platforms favor content that generates lots of clicks – and therefore ad dollars – whether the information is true or not. A typical version of this view came from **Jonathan Brewer**, consulting engineer for Telco2. He commented, "The incentives for social media providers are at odds with stemming the spread of misinformation. Outrageous claims and hyperbole will always generate more advertising revenue than measured analysis of an issue."

Gina Neff, professor at the Oxford Internet Institute, said, "The economic stakes are simply too high to rein in an information ecosystem that allows false information to spread. Without the political commitment of major social media platforms to address the problem, the technical challenges to solving this problem will never be met."

Ari Ezra Waldman, associate professor of law at the New York Law School, wrote, "The spread of misinformation will only improve if platforms take responsibility for their role in the process. So far, although intermediaries like Facebook have nodded toward doing something about 'fake news' and cyberharassment and other forms of misleading or harmful speech, they simultaneously continue to maintain that they are merely neutral conduits and, therefore, uneasy about maintaining any sort of control over information flow. The 'neutral conduit' canard is a socio-legal strategy that is little more than a fancy way of absolving themselves of responsibility for their essential role in the spread of misinformation and the decay of discourse."

Joseph Turow, professor of communication at the University of Pennsylvania, commented, "The issues of 'fake' and 'weaponized' news are too complex to be dealt with through automated, quantitative or algorithmic means. These activities have always existed under one label or another, and their rapid distribution by activist groups, companies and governments as a result of new technologies will continue. One reason is that the high ambiguity of these terms makes legislating against them difficult without infringing on speech and the press. Another reason is that the people sending out such materials will be at least as creative as those trying to stop them."

A **professor of legal issues and ethics at one of the pre-eminent graduate schools of business in the United States** said, "The basic incentive structure that promotes untrustworthy information flow won't change, and the bad guys will improve their approaches faster than the good guys."

Dave Burstein, editor of FastNet.news, said, "Speaking of reports on policy and technology, the important thoroughly misleading information usually comes from the government and especially lobbyists and their shills. All governments lie, I.F. Stone taught us, and I can confirm that's been true of both Obama's people and the Republicans this century I have reported. Corporate advocates with massive budgets – Verizon and AT&T in the hundreds of billions – bamboozle reporters and governments into false claims. The totally outnumbered public-interest advocates often go over the line sometimes as well."

Johanna Drucker, professor of information studies at the University of California, Los Angeles, commented, "The constructedness (sic) of discourse removes news from the frameworks in which verification can occur. Responsible journalism will continue on the basis of ethical accountability, but nothing will prevent other modes of discourse from proliferating. No controls can effectively legislate for accuracy or verity. It is a structural impossibility to suture language and the lived."

Mercy Mutemi, legislative advisor for the Kenya Private Sector Alliance, commented, "Fake news spreads faster than genuine news. It is more attractive and 'hot.' We do not see corresponding efforts from genuine news peddlers to give factual information that is timely and interesting. On the contrary, reporters have become lazy, lifting articles off social media and presenting only obvious facts. Fake news peddlers have invested resources (domains and bots) to propagate their agenda. There isn't a corresponding effort by genuine news reporters. People will get so used to being 'duped' that they will treat everything they read with skepticism, even real news. It will no longer be financially viable to invest in real news as the readership may go down. In such an environment, it is likely fake news will continue to thrive."

A **professor of media and communication** based in Europe said, "The online information environment will not improve if its architectural design, operation and control is left to five big companies alone. If they do not open up their algorithms, data governance and business models to allow for democratic and civic participation (in other words, if there is only an economic driver to rule the information environment) the platform ecosystem will not improve its conditions to facilitate an open and democratic online world."

A **leading researcher studying the spread of misinformation** observed, "The payoffs for actors who are able to set the agenda in the emerging information environment are rising quickly. Our collective understanding of and ability to monitor these threats and establish ground rules across disparate communities, geographies and end devices will be challenged."

A **research scientist at Oxford University** commented, "Misinformation and disinformation and motivated reasoning are integral to platform capitalism's business model."

Rick Hasen, professor of law and political science at the University of California, Irvine, said, "By 2027 there will be fewer mediating institutions such as acceptable media to help readers/viewers ferret out truth. And there will be more deliberate disinformation from people in and out of the U.S."

Raymond Hogler, professor of management at Colorado State University, replied, "Powerful state actors … will continue to disseminate false, misleading and ideologically driven narratives posing as 'news.'"

A **member of the Internet Architecture Board** said, "The online advertising ecosystem is very resistant to change, and it powers the fake news 'industry.' Parties that could do something about it (e.g., makers of browsers) don't have a strong incentive to do so."

A **professor of law at a state university** replied, "Powerful incentives will continue for irresponsible politicians and others in the political industry (paid or not) to spread false information and for publications to allow it to circulate: attention, clicks, ad revenue, political power. Meanwhile the First Amendment will protect [sharing of all information] powerfully inside the United States as the overall moral and ethical character of the country continues to be debased."

An **author/editor/journalist** wrote, "Confirmation bias, plus corporate manipulation, will not allow an improvement in the information environment."

An **internet pioneer and principal architect in computing science** replied, "Clicks will remain paramount, and whether those clicks are on pages containing disinformation or not will be irrelevant."

Edward Kozel, an entrepreneur and investor, predicted, "Although trusted sources (e.g., The New York Times) will remain or new ones will emerge, the urge for mass audience and advertising revenue will encourage widespread use of untrusted information."

David Schultz, professor of political science at Hamline University, said, "The social media and political economic forces that are driving the fragmentation of truth will not significantly change in the next 10 years, meaning the forces that drive misinformation will continue."

Paul Gardner-Stephen, senior lecturer at the College of Science & Engineering at Flinders University, noted, "Increasing technical capability and automation, combined with the demonstrated dividends that can be obtained from targeted fake news makes an arms race inevitable. Governments and political parties are the major players. This is Propaganda 2.0."

Peter Levine, associate dean and professor at the Tisch College of Civic Life at Tufts University, observed, "I don't think there is a big enough market for the kinds of institutions, such as high-quality newspapers, that can counter fake news, plus fake news pays."

A **postdoctoral scholar at a major university's center for science, technology and society** predicted, "Some advances will be made in automatically detecting and filtering 'fake news' and other misinformation online. However, audience attention and therefore the financial incentives are not aligned to make these benefits widespread. Even if some online services implement robust filtering and detection, others will happily fill the void they leave, pandering to a growing audience willing to go to 'alternative' sites to hear what they want to hear."

David Brake, a researcher and journalist, pointed out, "The production and distribution of inaccurate information has lower cost and higher incentives than its correction does."

Mark Lemley, a professor of law at Stanford University, wrote, "Technology cannot easily distinguish truth from falsehood, and private technology companies don't necessarily have the incentive to try."

Darel Preble, president and executive director at the Space Solar Power Institute, commented, "Even the technical media ... is substituting ad hominem attacks (or volume) and repetition for technical accuracy to complex problems. Few people are familiar with or want to risk their paycheck to see these problems fixed, so these problems will continue growing for now."

Amali De Silva-Mitchell, a futurist, replied, "There is political and commercial value in misinformation. Absolutely ethical societies have never existed. Disclosures are critical and it will be important to state the source of news as being human or machine, with the legal obligation remaining with the human controller of the data."

Some said the information environment is impossible to fully tame due to the human drive to continually innovate, competing to upgrade, monetize and find new ways to assert power.

Alan D. Mutter, media consultant and faculty at the graduate school of journalism at the University of California, Berkeley, replied, "The internet is, by design, an open and dynamically evolving platform. It's the Wild West, and no one is in charge."

Anonymous respondents commented:
- "'Fake news' is just the latest incarnation of propaganda in late capitalism."
- "The profit motive will be put in front of value. The reliance of corporations on algorithms that allow them to do better targeting leads to greater fragmentation and greater possibility for misinformation."
- "People have to use platforms for internet communication. The information environment is managed by the owners of these platforms who may not be so interested in ethical issues."
- "We cannot undo the technology and economics of the current information environment, nor can we force those who are profiting from misinformation to forego their monetary gains."

Human tendencies and infoglut drive people apart and make it harder for them to agree on 'common knowledge.' That makes healthy debate difficult and destabilizes trust. The fading of news media contributes to the problem

Many of these experts said one of the most serious problems caused by digital misinformation and the disruption of public support of traditional news media models is the shrinkage of the kind of commonly embraced facts that are the foundation of civil debate – a consensus understanding of the world. An **anonymous respondent** predicted, "The ongoing fragmentation of communities and the lack of common voice will lead to the lower levels of trust."

A **professor of education policy** commented, "Since there is no center around which to organize truth claims (fragmented political parties, social groups, identity groups, institutional affiliations, fragmentation of work environments, increasing economic

precarity, etc.) … there are likely to be more, not fewer, resources directed at destabilizing truth claims in the next 10 years."

An **historian and former legislative staff person based in North America** observed, "A major issue here is that what one side believes is true, is not the same as what the other side believes. Example: What Yankees and Confederates believed about the Civil War has never been the same, and there are differing social and cultural norms in different ages, times, regions and religions that have different 'takes' on what is right and proper behavior. We are facing an almost existential question here of 'what is truth?'"

Daniel Wendel, a research associate at MIT, said, "Trust is inherently personal. While central authorities can verify the identity of a particular website or person, consumers are less likely to trust a 'trusted' centralized fact checker [than the sources that express the same belief system as they and their friends]. For example, Snopes.com has already been discounted by right-wing pundits as being too 'liberal.' Trust must come from networks rather than authorities, but the ideas behind that are nascent and the technologies do not yet exist."

Philip Rhoades, retired IT consultant and biomedical researcher with the Neural Archives Foundation, said, "The historical trend is for information to be less reliable and for people to care less."

A **professor of rhetoric and communication** noted, "People can easily stay in their own media universe and never have to encounter ideas that conflict with their own. Also, the meshing of video and images with text creates powerful effects that appeal to the more rudimentary parts of the brain. It will take a long time for people to adapt to the new media environment."

A **professor of journalism at New York University** observed, "The fragmentation of the sources of media – and increasing audience participation – meant that it was no longer just canonical sources that could get their voices amplified."

A number of respondents challenged the idea that any individuals, groups or technology systems could or should "rate" information as credible or not.

A **professor of political economy at a U.S. university** wrote, "I don't think there is a clear, categorical distinction between 'false' news and the other kind. Some falsehoods have

been deliberately fostered by elites for purposes of political management – the scope has widened dramatically in recent years."

Greg Shatan, partner at Bortstein Legal Group based in New York, replied, "Unfortunately, the incentives for spreading false information, along with the incentives for destabilizing trust in internet-based information, will continue to incentivize the spread of 'fake news.' Perversely, heightened concerns about privacy and anonymity are counterproductive to efforts to increase trust and validation."

A **project manager for the U.S. government** responded, "It is going to get much worse before it gets better. There is no sign that people are willing to work at what we agree on, most would prefer to be divisive and focus on differences."

An **anonymous research scientist** said, "I do not buy the assumption that information, 'accurate' or not, is the basis of political or – in fact – any action. I actually think it never has been. Yes, this is the story we like to tell when justifying actions vis-a-vis everyone else. It helps us present ourselves as rational, educated and considerate human beings. But no, in practice we do and say and write and report whatever seems reasonable in the specific situation for the specific purposes at hand. And that is OK, as long as others have the opportunity to challenge and contest our claims."

Some respondents noted that trust has to be in place before people can establish any sort of shared knowledge or begin to debate and decide the facts on which decisions can be based.

An **anonymous internet activist/user based in Europe** commented, "Who can determine what is or is not fake news?"

A **principal research scientist based in North America** commented, "The trustworthiness of information is a subjective measure as seen by the consumer of that information."

An **anonymous futurist/consultant** said, "Technology and platform design is only one part of the problem. Building trust and spreading information-quality skills takes time and coordination."

A **director with a digital learning research unit at a major university on the U.S. West Coast** said, "As the technology evolves, we will find ways (technologically) and also culturally to become savvier about the way in which we manage and define 'trustworthiness.'"

**A small segment of society will find, use and perhaps pay a premium
for information from reliable, quality sources. Outside of this group
'chaos will reign' and a worsening digital divide will develop**

A deeper digital divide was predicted by some respondents who said that 10 years from now, those who value accurate information and are willing to spend the time and/or money to get it will separate from those who do not. **Alex 'Sandy' Pentland**, member of the U.S. National Academy of Engineering and the World Economic Forum, predicted of the information environment, "Things will improve, but only for the minority willing to pay subscription prices."

An **anonymous journalist** observed, "One of today's most glaring class divides is between those who are internet-savvy and so skilled at evaluating different sources and information critically that it's almost instinctive/automatic, and those who have very limited skills in that department. This divide is usually glaringly obvious in anyone's Facebook feed now that such a large portion of the population is on Facebook, and the lack of ability to evaluate sources online critically is most common in older persons with limited education and/or limited internet proficiency – and can sometimes also be observed in young people with the same attributes (limited education/internet proficiency)."

Garland McCoy, president of the Technology Education Institute, predicted, "As most of us know there is the public internet, which operates as a 'best effort' platform and then there are private internets that command a premium because they offer much more reliable service. So it will be with the 'news' and information/content on the internet. Those who have the resources and want fact checking and vetting will pay for news services, which exist today, that charge a subscription and provide, for the most part, vetted/authenticated facts 'news.' Those who do not have the resources or who don't see the 'market value' will take their chances exploring the world of uncensored, unfiltered and uncontrolled human mental exertion."

A **professor whose research is focused on this topic** wrote, "I can envisage [several] scenarios – trusted networks (where false information is pointed out), or the wild unbounded morass. It may well be that one will have to pay to join such a trusted network because those who can provide trusted information will be paid to do so."

Meamya Christie, user-experience designer with Style Maven Linx, replied, "There will be a division in how information is consumed. It will be like a fork in the road. People will have

a choice to go through one portal or another based on their own set of core values, beliefs and truths."

A **strategist for an institute** replied, "The trust in 2027 will be only for the elites who can pay, or for the most-educated people."

A **fellow at a UK-based university** said, "I don't think a technological or top-down solution can 'fix' the information environment without addressing a range of root issues relating to democratic disenfranchisement, deteriorating education and anti-intellectualism."

A **senior research fellow** working for the positive evolution of the information environment said, "Only a small fraction of the population (aged, educated, affluent – i.e., ready to pay for news) will have good, balanced, fair accurate, timely, contextualized, information."

Theme 2: The information environment will *not* improve because technology will create new challenges that can't or won't be countered effectively and at scale

Many respondents who expect no improvement in the information environment argue that certain actors in government, business and other individuals with propaganda agendas and special interests are turning technology to their favor in the spread of misinformation. There are too many of them and they are clever enough that they will continue to infect the online information environment, according to these experts.

A clear articulation of this view came from **Howard Greenstein**, adjunct professor of management studies at Columbia University. He argued, "This is an asymmetric problem. It is much easier for single actors and small groups to create things that are spread widely, and once out, are hard to 'take back.'" Moreover, the process of distinguishing between legitimate information and questionable material is very difficult, those who support this line of reasoning said.

An **anonymous respondent** wrote, "Whack-a-mole seems to be our future. There is an inability to prevent new ways of disrupting our information systems. New pathways will emerge as old ones are closed."

Those generally acting for themselves and not the public good have the advantage, and they are likely to stay ahead in the information wars

Eric Burger, research professor of computer science and director of the Georgetown Center for Secure Communications in Washington, D.C., replied, "Distinguishing between fake news, humor, strange-but-true news or unpopular news is too hard for humans to figure out, no less a computer."

Wendell Wallach, a transdisciplinary scholar focused on the ethics and governance of emerging technologies at The Hastings Center, wrote, "While means will be developed to filter out existing forms of misinformation, the ability to undermine core values will continue to be relatively easy while steps to remediate destructive activities will be much harder and more costly. Furthermore, a gap will expand as technological possibilities speed ahead of their ethical-legal oversight. Those willing to exploit this gap for ideological purposes and personal gain will continue to do so."

Justin Reich, assistant professor of comparative media studies at MIT, noted, "Strategies to label fake news will require algorithmic or crowd-sourced approaches. Purveyors of fake news are quite savvy at reverse engineering and gaming algorithms, and equally adept at mobilizing crowds to apply 'fake' labels to their positions and 'trusted' labels to their opponents."

Sean Goggins, an associate professor and sociotechnical data scientist, wrote, "Our technical capacity to manipulate information will continue to grow. With investment tilted toward for-profit enterprise and the intelligence community and away from public-sector research like that sponsored by the National Science Foundation, it's doubtful that technology for detecting misinformation will keep up with technologies designed to spread misinformation."

An **associate professor of communication studies at a Washington-based university** said, "The fake news problem is not one that can be fixed with engineering or technological intervention short of a total reimagination of communication network architecture."

Fredric Litto, professor emeritus at the University of São Paulo in Brazil, wrote, "The incredibly complex nature of contemporary information technology will inevitably make for a continuing battle to reduce (note: I dare not say eliminate) false and undesirable 'news' and other information permeating electronic media. Without a foolproof method of truly eliminating the possibility of anonymity – and I cannot see this really happening by 2027 – there will be no end to the malicious use of most, if not all, modes of communication."

Michel Grossetti, research director at CNRS (French National Center for Scientific Research), commented, "It is the old story of the bullet and the cuirass. Improvement on one side, improvement on the other."

Daniel Berleant, author of the book "The Human Race to the Future," predicted, "Digital and psychological technologies for the spreading of misinformation will continue to improve, and there will always be actors motivated to use it. Ways to prevent it will develop as well but will be playing catch-up rather than taking the lead."

John Lazzaro, a retired electrical engineering and computing sciences professor at the University of California, Berkeley, wrote, "I don't think society can reach a consensus on what constitutes misinformation, and so trying to automate the removal of misinformation won't be possible."

Andreas Birkbak, assistant professor at Aalborg University in Copenhagen, said, "The information environment will not improve because there is no way to automate fact checking. Facts are context-dependent."

A **North American program officer** wrote, "While technology may stop bots from spreading fake news, I don't think it will be that easy to stop people who want to believe the fake news and/or make up the fake news."

A **researcher based in North America** said, "News aggregators such as Facebook will get better at removing low-information content from their news feeds but the amount of mis/disinformation will continue to increase."

Joseph Konstan, distinguished professor of computer science and engineering at the University of Minnesota, observed, "Those trying to manipulate the public have great resources and ingenuity. While there are technologies that can help identify reliable information, I have little confidence that we are ready for widespread adoption of these technologies (and the censorship risks that relate to them)."

A **former software systems architect** replied, "Bad actors will always find ways to work around technical measures. In addition, it is always going to be human actors involved in the establishment of trust relationships and those can be gamed. I do not envision media organizations being willing participants."

Can technology detect and flag trustworthy information? A **North American research scientist** said the idea of basing likely veracity on people's previous information-sharing doesn't always work, writing, "People don't just share information because they think it's true. They share to mark identity. Truth-seeking algorithms, etc. don't address this crucial component."

A **vice president for an online information company** wrote, "It is really hard to automatically determine that some assertion is fake news or false. Using social media and 'voting' is overcome by botnets for example."

J. Cychosz, a content manager and curator for a scientific research organization, commented, "False information has always been around and will continue to remain, technology will emerge that will help identify falsehoods and culture will shift, but there will always be those who find a path around."

Philippa Smith, research manager and senior lecturer in new media at Auckland University of Technology, noted, "Efforts to keep pace with technology and somehow counteract the spread of misinformation or fake news may be more difficult than we imagine. I have concerns that the horse has bolted when it comes to trying to improve the information environment."

Frank Odasz, president of Lone Eagle Consulting, observed, "Having watched online scams of all kinds evolve to be increasingly insidious, I expect this trend will continue and our best cybersecurity will forever be catching up with, not eradicating [it]. The battle between good and evil is accelerated digitally."

Ed Terpening, an industry analyst with the Altimeter Group, replied, "Disinformation will accelerate, as trust in institutions we've thought of as unbiased widen polarization through either hiding or interpreting facts that fulfill an agenda."

Basavaraj Patil, principal architect at AT&T, wrote, "The rapid pace of technological change and the impact of false information on a number of aspects of life are key drivers."

Bradford W. Hesse, chief of the health communication and informatics research branch of the U.S. National Cancer Institute, said, "Communication specialists have been dealing with the consequences of propaganda, misinformation and misperceived information from before and throughout the Enlightenment. What has changed is the speed with which new anomalies are detected and entered into the public discourse. The same accelerated capacity will help move the needle on social discourse about the problem, while experimenting with new solutions."

Liam Quin, an information specialist at the World Wide Web Consortium, said the information environment is unlikely to be improved because "human nature won't change in such a short time, and people will find ways around technology."

Alan Inouye, director of public policy for the American Library Association, commented, "New technologies will continue to provide bountiful opportunities for mischief. We'll be in the position of playing defense as new abuses or attacks arise." However, he also added, "This will be a future that is, on balance, not worse than today's situation."

A distinguished engineer for a major provider of IT solutions and hardware warned that any sort of filtering system will flag, filter or delete useful content along with the

misinformation, "It's not possible to censor the untrustworthy news without filtering some trustworthy news. That struggle means the situation is unlikely to improve."

Weaponized narratives and other false content will be magnified by social media, online filter bubbles and AI

Some respondents noted that the people best served by the manipulation of public sentiment, arousing fear and anger and obfuscating reality, are encouraged by their success now and that gives them plenty of incentive to make things worse in the next decade. As a **professor and author based in the United States** put it, "Too many people have realized that lying helps their cause."

An **anonymous respondent based in Asia/Southeast Asia** replied, "We are being 'gamed,' simply put."

Alexis Rachel, user researcher and consultant, said, "The logical progression of things at this point (unless something radical occurs) is that there will be increasingly more 'sources' of information that are unverified and vetted – a gift from the internet and the ubiquitous publishing platform it is. All it takes is something outrageous and plausible enough to go viral, and once out there, it becomes exceedingly difficult to extinguish – fact or fiction."

Martin Shelton, a security researcher with a major technology company, said, "Just as it's now straightforward to alter an image, it's already becoming much easier to manipulate and alter documents, audio and video, and social media users help these fires spread much faster than we can put them out."

Matt Stempeck, a director of civic technology, noted, "The purveyors of disinformation will outpace fact-checking groups in both technology and compelling content unless social media platforms are able to stem the tide."

Alf Rehn, chair of management and organization studies at Åbo Akademi University, commented, "Better algorithms will sort out some of the chaff [and may improve the overall information environment] but at the same time the weaponization of fake news will develop. As strange as it seems, we may enter a time of less, but 'better' [more effective] fake news."

An **anonymous respondent,** wrote, "Distrust of academics and scientists is so high it's hard to imagine how to construct a fact-checking body that would trusted by the broader population."

The most-effective tech solutions to misinformation will endanger people's dwindling privacy options, and they are likely to limit free speech and remove the ability for people to be anonymous online

While some people believe more surveillance and requirements for identity authentication are go-to solutions for reining in the negative impacts of misinformation, a number of these experts said bad actors will evade these measures and platform providers, governments and others taking these actions will expand unwanted surveillance and curtail civil liberties.

Fred Davis, a futurist based in North America, wrote, "Automated efforts to reduce fake news will be gamed, just like search is. That's 20 years of gaming the system – search engine optimization and other things that corrupt the information discovery process have been in place for over 20 years, and the situation is still bad. Also, it may be difficult to implement technology because it could also be used for mass censorship. Mass censorship would have a very negative effect on free speech and society in general."

Adam Powell, project manager at the Internet of Things Emergency Response Initiative at the University of Southern California, said, "The democratization of the internet, and of information on the internet, means just that: Everyone has and will have access to receiving and creating information, just as at a watercooler. Not only *won't* the internet suddenly become 'responsible,' it shouldn't, because that is how totalitarian regimes flourish (see: Firewall, Great, of China)."

An **eLearning specialist** observed, "Any system deeming itself to have the ability to 'judge' information as valid or invalid is inherently biased." And a **professor and researcher** noted, "In an open society, there is no prior determination of what information is genuine or fake."

The **owner of a consultancy** replied, "We're headed to a world where most people will use sources white-listed (explicitly or not) by third parties (e.g., Facebook, Apple, etc.)."

A **distinguished professor emeritus of political science at a U.S. university** wrote, "Misinformation will continue to thrive because of the long (and valuable) tradition of freedom of expression. Censorship will be rejected."

A **professor at a major U.S. university** replied, "Surveillance technologies and financial incentives will generate greater surveillance." A **retired university professor** predicted, "Increased censorship and mass surveillance will tend to create official 'truths' in various

parts of the world. In the United States, corporate filtering of information will impose the views of the economic elite."

Among the respondents to this canvassing who recommended the removal of anonymity was **Romella Janene El Kharzazi**, a content producer and entrepreneur, who said, "One obvious solution is required authentication; fake news is spread anonymously and if that is taken away, then half of the battle is fought and won." A **research scientist based in Europe** predicted, "The different actors will take appropriate measures – including efficient interfaces for reporting and automatic detection – and implement efficient decision mechanisms for the censorship of such content."

A **senior researcher and distinguished fellow for a major futures consultancy** observed, "Reliable fact checking is possible. Google in particular has both the computational resources and talent to successfully launch a good service. Facebook may also make progress, perhaps in a public consortium including Google. Twitter is problematic and would need major re-structuring including a strict, true names policy for accounts – which is controversial among some privacy sectors."

A **retired consultant and strategist for U.S. government organizations** replied, "Regardless of technological improvements, the change agents here are going to have to be, broadly speaking, U.S. Supreme Court judges' rulings on constitutional interpretations of free speech, communication access and any number of other constitutional issues brought to the fore by many actors at both the state and national level, and these numerous judicial change agents' decisions are, in turn, affected by the citizen opinion and behavior."

Anonymous respondents also commented:
- "The means and speed of dissemination have changed [the information environment]. It cannot be legislated without limiting free speech."
- "It's impossible to filter content without bias."
- "The internet is designed to be decentralized; not with the purpose of promoting accuracy or social order."
- "There is no way – short of overt censorship – to keep any given individual from expressing any given thought."
- "Blocking (a.k.a. censoring) information is just too dangerous."
- "I do not think it can be stopped without doing a lot of damage to freedom of speech."
- "Forces of evil will get through the filters and continue to do damage while the majority will lose civil rights and many will be filtered or banned for no good reason."
- "It's a hard problem to solve fairly."

Theme 3: The information environment *will* improve because technology will help label, filter or ban misinformation and thus upgrade the public's ability to judge the quality and veracity of content

Many respondents who said they hope for or expect an improvement in the information environment 10 years from now mentioned ways in which new technological and verification solutions might be implemented. A number of these proposed solutions include the hope that technology will be created to evaluate content – making it "accessible."

Andrea Forte, associate professor at Drexel University, said, "As mainstream social media take notice of information quality as an important feature of the online environment, there will be a move towards designing for what I call '*assessability*' – interfaces that help people appropriate assessments of information quality."

Filippo Menczer, professor of informatics and computing at Indiana University, noted, "Technical solutions can be developed to incorporate journalistic ethics into social media algorithms, in a way similar to email spam filters."

Scott Fahlman, professor emeritus of AI and language technologies at Carnegie Mellon University, commented, "For people who are seriously trying to figure out what to believe, there will be better online tools to see which things are widely regarded as true and which have been debunked."

Robert Bell, co-founder of the Intelligent Community Forum, commented, "Technology moves fast and humans adapt more slowly, but we have a proven capability to solve problems we create with technology."

Joanna Bryson, associate professor and reader at University of Bath and affiliate with the Center for Information Technology Policy at Princeton University, responded, "We are in the information age, and I believe good tools are likely to be found in the next few years."

David J. Krieger, director of the Institute for Communication & Leadership in Lucerne, Switzerland, commented, "The information environment will improve because a data-driven society needs reliable information, and it is possible to weed out the false information."

Andrew McStay, professor of digital life at Bangor University in Wales, wrote, "Undoubtedly, fake news and weaponised information will increase in sophistication, but so will attempts to combat it. For example, the scope to analyse at the level of metadata is a promising opportunity. While it is an arms race, I do not foresee a dystopian outcome."

Clifford Lynch, director of the Coalition for Networked Information, noted, "The severity of the problem has now been recognized fairly widely, and while I expect an ongoing 'arms race' in the coming decade, I think that we will make some progress on the problem."

A **CEO and research director** noted, "There are multiple incentives, economic and political, to solve the problem."

An **anonymous respondent** said, "The public will insist that online platforms take more responsibility for their actions and provide more tools to ensure information veracity."

Likely tech-based solutions include adjustments to algorithmic filters, browsers, apps and plug-ins and the implementation of "trust ratings"

Matt Mathis, a research scientist at Google, responded, "The missing concept is an understanding of the concept of 'an original source.' For science, this is an experiment, for history (and news) an eyewitness account by somebody who was (verifiably) present. Adding 'how/why we know this' to non-original sources will help the understanding that facts are verifiable."

Federico Pistono, entrepreneur, angel investor and researcher with Hyperloop TT, commented, "Algorithms will be tailored to optimize more than clicks – as this will be required by advertisers and consumers alike – and deep learning approaches will improve."

Tatiana Tosi, netnographer at Plugged Research, commented, "The information environment will improve due to new artificial-intelligence bots that will verify the information. This should balance privacy and human rights in the automated environment."

A **web producer/developer for a U.S.-funded scientific agency** predicted, "The reliance on identity services for real-world, in-person interactions, which start with trust in web-based identification, will force reliability of information environments to improve."

An **associate professor of business** at a university in Australia commented, "Artificial intelligence technologies are advancing quickly enough to create an 'Integrity Index' for news

sources even down to the level of individual commentators. Of course, other AI engines will attempt to game such a system. I can envisage an artificial blogger that achieves high levels of integrity before dropping the big lie just in time for an election. Big lies take a day or more to be disproven so it may just work, but the penalty for a big lie, or any lie, can be severe so everyone who gained from the big lie will be tainted."

A **distinguished engineer for one of the world's largest networking technologies companies** commented, "Certificate technologies already exist to validate a website's sources and are in use for financial transactions. These will be used to verify sources for information in the future. Of course, there will always be people who look for information (true or false) that validates their biases."

Ayaovi Olevie Kouami, chief technology officer at the Free and Open Source Software Foundation for Africa, said, "The actual framework of the internet ecosystem could have a positive impact on the information environment by setting up all the requisite institutions, beginning with DNSSEC, IXPs, FoE, CIRT/CERT/CSIRT, etc."

Jean Paul Nkurunziza, a consultant based in Africa, commented, "The expected mass adoption of the IPv6 protocol will allow every device to have a public IP address and then allow the tracking of the origin of any online publication."

Mark Patenaude, vice president for innovation, cloud and self-service technology at ePRINTit Cloud Technology, replied, "New programming tech and knowledge will create a new language that will teach us to recognize malicious, false, misleading information by gathering all news and content sources and providing us with accurate and true information."

Hazel Henderson, futurist and CEO of Ethical Markets Media, said, "Global ethical standards and best practices are being developed in the many domains affected. New verification technologies, including blockchain and smart contracts, will help."

An **anonymous respondent based in North America** who has confidence things may be improved listed a series of technologies likely to be effective, writing: "Artificial intelligence, machine learning, exascale computing from everywhere, quantum computing, the Internet of Things, sensors, big data science and global collaborative NREN (National Research and Education Network) alliances."

An **anonymous respondent based in Europe** warned, "Technical tools and shields to filter and recognize manipulations will be more effective than attempts at education in critical thinking for end users."

Anonymous survey participants also responded:
- "Relatively simple steps and institutional arrangements can minimize the malign influence of misinformation."
- "Machines are going to get increasingly better at validating accuracy of information and will report on it."
- "Artificial intelligence technologies will advance a lot, making it easy to make fake news more difficult to be discovered and identified."
- "Technology for mass verification should improve as will the identification of posters. Fakers will still exist but hopefully the half-life of their information will shrink."
- "Things will improve due to [better tracking of the] provenance of data and security and privacy laws."

Regulatory remedies could include software liability law, required identities and the unbundling of social networks like Facebook

A number of respondents said that evidence suggests people and internet content platform providers can't solve this problem and argued there will be pressure for regulatory reforms that hold consistently bad actors responsible.

An **associate professor at a major Canadian university** said, "As someone who has followed the information-retrieval community develop over the past 15 years – dealing with spam, link farms, etc. – given a strong enough incentive, technologies will advance to address the challenge of misinformation. This may, however, be unevenly distributed, and may be more effective in domains such as e-business where there is a financial incentive to combat misinformation."

An **anonymous respondent** wrote, "I hope regulators will recognise that social media companies are publishers, not technology companies, and therefore must take responsibility for what they carry. Perhaps then social media companies will limit the publication of false advertising and misinformation."

A **professor of media and communication based in Europe** said, "It will be very difficult to assign penalties to culprits when platforms deny responsibility for any wrongdoing by their 'users.' Accountability and liability should definitely be assumed by

platform operators who spread news and information, regardless of its source and even if unwittingly. Government has very limited power to 'fake news' or 'misinformation' but it can definitely help articulate which actors in society are responsible."

A **senior vice president for government relations** predicted, "Governments should and will impose additional obligations on platforms to increase their responsibility for content on their services."

One possibility that a notable share of respondents mentioned is the requirement of an authenticated ID for every user of a platform. An **anonymous respondent** said, "Bad actors should be banned from access, but this means that a biography or identification of some sort would be necessary of all participants."

Those in support of requiring internet users to provide a real identity when participating online also mentioned the establishment of a reputation system. A **partner in a services and development company based in Switzerland** commented, "A bad reputation is the best penalty for a liar. It is the job of society to organize itself in a way to make sure that the bad reputation is easily visible. It should also extend to negligence and any other related behaviour allowing the spread of misinformation. Penal law alone is too blunt a tool and should not be regarded as a solution. Modern reputation tools (similar in approach to what financial audits and ratings have achieved in the 20th century) need to be built and their use must become an expected standard (just like financial audits are now a legal requirement)."

An **anonymous activist/user** wrote, "Loss of anonymity might be a way of ensuring some discipline in the system, yet the institutions which would be deciding such punishments today have no credibility with most of the population."

An **anonymous ICT for development consultant and retired professor** commented, "Government best plays a regulating role and laws are punitive; so both regulation and laws should be stringently applied."

A **post-doctoral fellow at a center for governance and innovation** replied, "Jail time and civil damages should be applied where injuries are proven. Strictly regulate non-traditional media especially social media."

An **associate professor at Brown University** wrote, "Essentially we are talking about the regulation of information, which is nearly impossible since information can be produced by anyone. Government can establish ethical guidelines, perhaps similar to the institutional

review boards that regulate scientific research. Or it can be done outside government, like a better business bureau."

An **anonymous respondent based in Europe** wrote, "Publicity, monetary fines and definitely jail terms, depending on the scope and consequences of the spreading false information. In terms of the government role in terms of prevention, it should not be different than any other area, including sound legal regulation, strengthened capacities identify false information and stop at early stages using legal mechanism, education and awareness raising of citizens, as well as higher ethical stands (or zero tolerance) for public officials walking on the edge."

A **postdoctoral scholar based in North America** wrote, "If we are talking about companies such as Facebook, I do think there is room for discussion on the federal level of their responsibility as, basically, a private utility. Regulation shouldn't be out of the question."

A **legal researcher based in Asia/Southeast Asia** said, "Stop them from using any internet. Government should create regulations for internet companies to prevent the distribution of false information."

A **professor of humanities** said, "Penalties are a nice idea, but who will decide which instances of 'fake news' require greater penalties than others? The bureaucracy to make these decisions would have to be huge."

Theme 4: The information environment *will* improve because people will adjust and make things better

Most respondents who expect an improvement in the information environment in the coming years put their faith in maturing – and more discerning – information consumers finding ways to cope personally and band together to effect change.

Alexios Mantzarlis, director of the International Fact-Checking Network based at the Poynter Institute for Media Studies, commented, "While the risk of misguided solutions is high, lots of clever people are trying to find ways to make the online information ecosystem healthier and more accurate. I am hopeful their aggregate effect will be positive."

Barry Chudakov, founder and principal at Sertain Research and StreamFuzion Corp., observed, "Globally, we have more people with more tools with more access to more information – and yes, more conflicting intent – than ever before; but, while messy and confusing, this will ultimately improve the information environment. We will continue to widen access to all types of information – access for citizen journalists, professionals, technical experts, others – so while the information environment becomes more diverse, the broader arc of human knowledge bends towards revelation and clarity; only mass suppression will stop the paid and unpaid information armies from discovering and revealing the truth."

A **North American research scientist** replied, "I'm an optimist, and believe we are going through a period of growing pains with the spread of knowledge. In the next decade, we'll create better ways to suss out truth."

Sharon Tettegah, professor at the University of Nevada, commented, "As we learn more about the types of information, we will be able to isolate misinformation and reliable sources."

Pamela Rutledge, director of the Media Psychology Research Center, noted, "Fake news and information manipulation are no longer 'other people's problems.' This new awareness of the importance of media will shift resources, education and behaviors across society."

Dariusz Jemielniak, professor of organization studies in the department of management in networked and digital societies (MiNDS) at Kozminski University, said, "There are a number of efforts aimed at eliminating fake news, and we as a society are going to make them work."

Misinformation has always been with us and people have found ways to lessen its impact. The problems will become more manageable as people become more adept at sorting through material

Many respondents said the online realm as simply yet another step in human and communications evolution and that history's lessons here should be comforting. They argued that previous information revolutions have inspired people to invent new ways to handle problems with information overload, the proliferation of misinformation, and opportunities for schemers to manipulate the emerging systems. The more hopeful among these experts believe that dynamic will play out again in the digital age.

A **professor of media studies** at a European university wrote, "The history of technology shows repeatedly that as a new technology is introduced – whatever the intentions of the designers and manufacturers, bad actors will find ways to exploit the technology in darker, more dangerous ways. In the short run, they can succeed, sometimes spectacularly: in the long run, however, we usually find ways to limit and control the damage."

A **futurist/consultant** replied, "We're seeing the same kinds of misinformation that used to be in supermarket tabloids move online – it's the format that has changed, not the human desire for salacious and dubious news."

Robin James, an associate professor of philosophy at a North American university, wrote, "The original question assumes that things have recently gotten worse. Scholars know that phenomena like patriarchy and white supremacy have created 'epistemologies of ignorance' that have been around for hundreds of years. 'Fake news' is just a new variation on this."

The **dean of one of the top 10 journalism and communications schools in the United States** replied, "Society always adjusts to new media and responds to weaknesses and flaws. Individuals will adjust, as will the technology."

Lokman Tsui, assistant professor at the School of Journalism and Communication at The Chinese University of Hong Kong, commented, "The information environment will improve. This is not a new question; we had concerns about fake news when radio broadcasting and mass media first appeared (for example, the Orson Welles' reading of 'War of the Worlds'). People will develop literacy. Standards, norms and conventions to separate advertising from 'organic' content will develop. Bad actors who profit from fake news will be identified and targeted."

Adam Nelson, a developer at Amazon, replied, "We had yellow journalism a hundred years ago and we have it now. We're at a low point of trust, but people will begin to see the value of truth once people become more comfortable with what social platforms do and how they work."

Axel Bruns, professor at the Digital Media Research Centre at the Queensland University of Technology, commented, "Moral panics over new media platforms are nothing new. The web, television, radio, newspapers and even the alphabet were seen as making it easier to spread misinformation. The answer is media literacy amongst the public, which always takes some years to catch up with the possibilities of new media technologies."

An **anonymous respondent** who predicts improvement replied, "Powerful social trends have a life cycle, and the pendulum typically swings back over time."

An **anonymous respondent** said, "It is the nature of the technical development that politics and regulatory forces are only able to react ex post, but they will."

A **senior researcher at a U.S.-based nonprofit research center** replied, "The next generation of news and information users will be more attuned to the environment of online news and will hopefully be more discerning as to its veracity. While there are questions as to whether the digital native generation can accurately separate real news from fake, they at least will have the technical and experiential knowledge that the older generations mostly do not."

Many respondents expressed faith that technologists would be at the forefront of helping people meet the challenges of misinformation.

A **managing partner and fellow in economics** predicted, "In order to avoid censorship, the internet will remain relatively open, but technology will develop to more effectively warn and screen for fact-inaccurate information. Think of it as an automated 'PolitiFact' that will point out b******* passively to the reader."

An **author and journalist based in North America** said, "Social media, technology and legacy media companies have an ethical and economic incentive to place a premium on trusted, verified news and information. This will lead to the creation of new digital tools to weed out hoaxes and untrusted sources."

Susan Price, lead experience strategist at Firecat Studio, observed, "There will always be a demand for trusted information, and human creativity will continue to be applied to create solutions to meet that demand."

Dane Smith, president of the public policy research and equity advocacy group Growth & Justice, noted, "I'm an optimist. Truth will find a way and prevail."

Louisa Heinrich, founder of Superhuman Ltd., commented, "The need to tell our stories to one another is a deeply rooted part of human nature, and we will continue to seek out better ways of doing so. This drive, combined with the ongoing upward trend of accessibility of technology, will lead more people to engage with the digital information environment, and new trust frameworks will emerge as old ones collapse."

Michael R. Nelson, public policy executive at Cloudflare, replied, "Some news sites will continue to differentiate themselves as sources of verified, unbiased information, and as these sites learn how to better distinguish themselves from 'fake news' sites, more and more advertisers will pay a premium to run their ads on such sites."

Steven Polunsky, writer with the Social Strategy Network, replied, "As with most disruptive events, people will adjust to accommodate needs and the changing environment."

Liz Ananat, an associate professor of public policy and economics at a major U.S. university wrote, "It will likely get worse first, but over 10 years, civil society will respond with resources and innovation in an intensive effort. Historically, when civil society has banded together and given its all to fight destructive forces, it has been successful."

Jane Elizabeth, senior manager at the American Press Institute, said, "The information environment will improve because the alternative is too costly. Misinformation and disinformation will contribute to the crumbling of a democratic system of government."

A number of these respondents said they expect information platform providers to police the environment in good faith, implementing the screening of content and/or other solutions while still protecting rights such as free speech.

A **principal network architect for a major edge cloud platform company** replied, "Retooling of social networking platforms will likely, over time, reduce the value of stupid/wrong news."

A **senior solutions architect for a global provider of software engineering and IT consulting services** wrote, "The problem of fake news is largely a problem of untrusted source. Online media platforms delegated the role of human judgment to algorithms and bots. I expect that these social media platforms will begin to exercise more discretion in what is posted when."

An **anonymous respondent** said, "Information platforms optimized for the internet are in their infancy. Like early e-commerce models, which merely sought to replicate existing, known systems, there will be massive shifts in understanding and therefore optimizing new delivery platforms in the future."

An **anonymous respondent** wrote, "Google and other outlets like Facebook are taking measures to become socially responsible content promoters. Combined with research trends in AI and other computing sectors, this may help improve the 'fake news' trends by providing better attribution channels."

Adam Gismondi, a researcher at the Institute for Democracy & Higher Education at Tufts University, predicted, "Ultimately, the information distributors – primarily social media platform companies, but others as well – will be forced, through their own economic self-interest and public pushback, to play a pivotal role in developing filters and signals that make the information environment easier for consumers to navigate."

Anonymous respondents shared these related remarks:
- "Everything we know about how human ingenuity and persistence has shaped the commercial and military (and philanthropic) drivers of the internet, and the web suggests to me that we will continue to ensure this incredible resource remains useful and beneficial to our development."
- "The tide of false information has to be stemmed. The alternative will be dystopia."
- "People will gain in sophistication, especially after witnessing the problems caused by the spread of misinformation in this decade. Vetting will be more sophisticated, and readers/viewers will be more alert to the signs that a source is not reliable."
- "I have hope in human goodness."
- "Over the next 10 years, users will become much more savvy and less credulous on average."
- "People will develop better practices for dealing with information online."

Crowdsourcing will work to highlight verified facts and block those who propagate lies and propaganda. Some also have hopes for distributed ledgers (blockchain)

Some respondents expressed optimism about the potential for people's capabilities in improving the visibility of the most-useful content, including the implementation of human-machine evaluation of content to identify sources, grade their credibility and usefulness, and possibly flag, tag or ban propagators of misinformation. An **anonymous respondent** wrote, "AI, blockchain and crowdsourcing appear to have promise."

An **assistant professor at a university in the U.S. Midwest** wrote, "Crowd-based systems show promise in this area. Consider some Reddit forums where people are called out for providing false information … if journalists were called out/tagged/flagged by large numbers of readers rather than their bosses alone, we would be inching the pebble forward."

But whose "facts" are being verified in this setting? **Ned Rossiter**, professor of communication at Western Sydney University, argued, "Regardless of advances in verification systems, information environments are no longer enmeshed in the era of broadcast media and national publics or 'imagined communities' on national scales. The increasing social, cultural and political fragmentation will be a key factor in the ongoing contestation of legitimacy. Informational verification merely amplifies already existing conditions."

Richard Rothenberg, professor and associate dean at the School of Public Health at Georgia State University, said, "It is my guess that the dark end of the internet is relatively small but it has an outsized presence. … If nothing else, folks have demonstrated enormous resourcefulness, particularly in crowd endeavors, and I believe methods for assuring veracity will be developed."

An anonymous **research scientist based in North America** wrote, "A system that enables commentary on public assertions by certified, non-anonymous reviewers – such that the reviewers themselves would be subject to Yelp-like review – might work, with the certification provided by Verisign-like organizations. Wikipedia is maybe a somewhat imperfect prototype for the kind of system I'm thinking of."

A **Ph.D. candidate in informatics**, commented, "It is possible to create systems that are reliable and trusted, but probably not unhackable. I imagine there could be systems that

leverage the crowd to check facts in real time. Computational systems would be possible, but it would be very difficult to create algorithms we could trust."

Jack Park, CEO at TopicQuests Foundation, predicted, "There will be new forms of crowdsourcing – a radical kind of curation – participation in which will improve critical-thinking skills and will mitigate the effects of misinformation."

Some respondents also pointed out the rise of additional platforms where people can publish useful information could be a positive force. An **anonymous respondent** wrote, "The rise of more public platforms for media content (online opinion/editorials and platforms such as Medium) gives me confidence that as information is shared, knowledge will increase so that trust and reliability will grow. Collaboration is key here."

Blockchain systems were mentioned by a number of respondents – a **senior expert in technology policy based in Europe**, commented, "… use blockchain to verify news" – but with mixed support, as many hedged their responses. A **journalist who writes about science and technology** said, "We can certainly create blockchain-like systems that are pretty reliable. Nothing is ever perfect, though, and trusted systems are often hard to use."

The **president** of a center for media literacy commented, "The technology capability [of potential verification systems] is immature and the costs are high. Blockchain technology offers great promise and hope."

A **journalist and experience strategist** at one of the world's top five technology companies said, "The blockchain can be used to create an unhackable verification system. However, this does not stop the dissemination of 'fake news,' it simply creates a way to trace information."

A **chief executive officer** said, "Can P2P, blockchain, with attribution be unhackable? We need a general societal move to more transparency."

Theme 5: Tech can't win the battle. The public must fund and support the production of objective, accurate information. It must also elevate information literacy to be a primary goal of education

A large share of respondents said that technology alone can't work to improve the information environment. Among these respondents, most pointed out two areas of concern: 1) The need for better funding of and support for journalism that serves the common good. The attention economy of the digital age does not support journalism of the general quality of the news media of the late 20th century, which was fairly well-respected for serving the public good with information that helped create an informed citizenry capable of informed decisions; 2) The need for massive efforts to imbue the public with much better information literacy skills; this requires an education effort that reaches out to those of all ages, everywhere.

Funding and support must be directed to the restoration of a well-fortified, ethical and trusted public press

Many respondents said the information environment can't be improved without more well-staffed, financially stable, independent news organizations capable of rising above the clamor of false and misleading content to deliver accurate, trusted content.

Susan Landau, a North American scientist/educator, wrote, "The underlying question is whether this dissemination will expand or not lies with many players, many in the private sector. How will the press handle 'fake news'? How will the internet companies do so? And how will politicians, at least politicians post-Trump? The rise of 'fake news' is a serious threat to democracy. Post-election [U.S. 2016], some in the press have been pursuing news with the same care and incisiveness that we saw in the Watergate era, but others are not. We have a serious threat here, but it is not clear that interests are aligned in responding to it. And it is not cheap to do so: securing sites against hacking is very difficult when the threat comes from a powerful nation state. Is there a way to create trusted, unhackable verification systems? This depends on what the use case is; it is a not 0-1 answer, but an answer in scales of grey. … If society cannot adequately protect itself against the co-opting of public information by bad actors, then democracy itself is in serious risk. We have had this problem for quite some time. … What has changed is the scope and scale of these efforts, partially through domestic funding, partially through foreign actors and partially through the ability of digital technologies to change the spread of 'false news.' What is needed to protect society against

the coopting of public information is not only protecting the sources of the information, but also creating greater public capability to discern nonsense from sense. … I do not see a role for government in preventing the spread of 'fake news' – that comes too close to government control of speech – but I do see one for government in preventing tampering with news and research organizations, disrupting flows of information, etc."

Timothy Herbst, senior vice president at ICF International, noted, "We have no choice but to come up with mechanisms to improve our information environment. The implications of not doing so will further shake trust and credibility in our institutions needed for a growing and stable democracy. Artificial intelligence (AI) should help but technological solutions won't be enough. We also need high-touch solutions and a reinforcement of norms that value accuracy to address this challenge."

Peter Jones, associate professor in strategic foresight and innovation at OCAD University in Toronto, predicted, "By 2027 decentralized internet services will displace mainstream news, as corporate media continues to erode trust and fails to find a working business model. Field-level investigative journalism will be crowdfunded by smaller consortiums, as current news organizations will have moved into entertainment, such as CNN already has."

A **senior international communications adviso**r commented, "I don't believe that the next 10 years will yield a business model that will replace the one left behind – particularly with respect to print journalism, which in the past offered audiences more in-depth coverage than was possible with video or radio. Today, print journalists effectively work for nothing [and] are exposed to liability and danger that would have been unheard of 25 years ago. Moreover, the separation between the interests of those corporations interested in disseminating news and editorial has all but closed – aside from a few noteworthy exceptions. Moreover, consumers of media appear to be having a harder time distinguishing spurious from credible sources – this could be the end result of decades of neglect regarding the public school system, a growing reliance on unsourced and uncross-checked social media or any number of other factors. Bottom line is that very few corporations seem willing [to] engage in a business enterprise that has become increasingly unfeasible from a financial point of view."

A **futurist/consultant based in Europe** said, "News has always been biased, but the apparent value of news on the internet has been magnified and so the value of exploiting it has also increased. Where there is such perceived value, the efforts to generate misleading news, false news and fake news will increase."

An **anonymous respondent** wrote, "There are too many pressures from the need to generate 'clicks' and increase advertising revenue."

There were complaints about news organizations in survival mode that neglect their role of informing the public in favor of pandering to it to stay afloat. Other experts worried about the quality of reporting in an age when newsrooms have been decimated.

An **anonymous respondent** wrote, "The talent pool the media system draws its personnel from will further deteriorate. Media personnel are influenced by defective information, and – even more – the quality of inferences and interpretations will decrease."

Some expressed concerns about finding unbiased details about the world in an online environment that becomes more cluttered all the time with content that does not feature this. An **anonymous survey participant** wrote, "I worry that sources of information will proliferate to the point at which it will be difficult to discern relatively unbiased sources from sources that are trying to communicate a point of view independent of supporting facts."

Thomas Frey, executive director and senior futurist at the DaVinci Institute, replied, "The credibility of the journalism industry is at stake and the livelihood of many people is hanging in the balance of finding the tools, systems and techniques for validating the credibility of news."

Eileen Rudden, co-founder of LearnLaunch, wrote, "The lack of trust in established institutions is at the root of the issue. Trust will need to be re-established."

An **international internet policy expert** said, "Demand for trusted actors will rise."

This is not an easy fix, by any means. **Kelly Garrett**, associate professor in the School of Communication at Ohio State University, said, "Although technology has altered how people communicate, it is not the primary source of distrust in authority, expertise, the media, etc. There are no simple technical solutions to the erosion of trust in those who produce and disseminate knowledge."

Rob Lerman, a retired information science professional, commented, "The combination of an established media which has encouraged opinion-based 'news.' The relative cheapness of websites, the proliferation of state-based misinformation and the seeming laziness of news consumers seems like an insurmountable obstacle to the improvement of the information environment."

Elevate information literacy: It must become a primary goal at all levels of education

A number of participants in this canvassing urged an all-out effort to expand people's knowledge about the ways in which misinformation is prepared and spread – an education in ways they can be wise and well-informed citizens in the digital age.

Jeff MacKie-Mason, university librarian and professor of information science and economics at the University of California, Berkeley, commented, "One wonder of the internet is that it created a platform on which essentially anyone can publish anything, at essentially zero cost. That will become only more true. As a result, there will be a lot of information pollution. What we must do is better educate information consumers and provide better systems for reputation to help us distinguish the wheat from the chaff."

Sharon Roberts, a Ph.D. candidate, wrote, "Social changes will be the ones that affect our perception of the information environment. Just like there are still 1-888 psychic call lines content on television or 'Nigerian princes' promising money sending me email, it's a social understanding of those meanings to be scams that have curtailed their [proliferation].'"

Sharon Haleva-Amir, lecturer in the School of Communication at Bar Ilan University in Israel, said, "I fear that the phenomenon of fake news will not improve due to two main reasons: 1) There are too many interested actors in this field (both business and politics wise) who gain from dispersion of false news and therefore are interested in keeping things the way they are; 2) Echo chambers and filter bubbles will continue to exist as these attitudes are typical to people's behavior offline and online. In order to change that, people will have to be educated since early childhood about the importance of both [the] credibility of sources as well as variability of opinions that create the market of ideas."

Sandra Garcia-Rivadulla, a librarian based in Latin America, replied, "It will be more important to educate people to be able to curate the information they get more effectively."

Jacqueline Morris, a respondent who did not share additional personal details, replied, "I doubt there will be systems that will halt the proliferation of fake news. … The only way is to reduce the value of fake news by ensuring that people do not fall for it, basically, by educating the population."

Mike O'Connor, a self-employed entrepreneur, wrote, "The internet is just like real life; bad actors will find ways to fool people. Healthy skepticism will be part of the mix."

Tomslin Samme-Nlar, technical lead at Dimension Data in Australia, commented, "I expect the information environment to improve if user-awareness programs and campaigns are incorporated in whatever solutions that are designed to combat fake news."

Geoff Scott, CEO of Hackerati, commented, "This isn't a technical or information problem; it's a social problem. Fake news works because it supports the point of view of the people it targets, which makes them feel good, right or vindicated in their beliefs. It takes critical thinking to overcome this, which requires effort and education."

Andreas Vlachos, lecturer in artificial intelligence at the University of Sheffield, commented, "I believe we will educate the public to identify misinformation better."

Iain MacLaren, director of the Centre for Excellence in Learning & Teaching at the National University of Ireland, Galway, commented, "The fact that more people are now fully aware of the existence of fake news, or propaganda, as it used to be known, means that there is increasing distrust of unverified/unrecognised providers of news and information. … I would like to hope, therefore, that a more sophisticated, critical awareness is growing across society, and I certainly hear much to that effect amongst the young people/students I work with. This also shows the importance of education."

Greg Wood, director of communications planning and operations for the Internet Society, replied, "The information environment will remain problematic – rumors, false information and outright lies will continue to propagate. However, I have hope that endpoints (people) can become more sophisticated consumers and thus apply improved filters. The evolution of email spam and how it has been dealt with provides a rough analogy."

Some people said, though, that information-literacy efforts, while possibly somewhat helpful in some cases, will not have an effect in many situations.

Sam Punnett, research officer at TableRock Media, replied, "The information environment will improve but what will determine this will be a matter of individual choice. Media literacy, information literacy, is a matter of choosing to be educated."

David Manz, a cybersecurity scientist, replied, "Technology exists and will be created to attribute statements to their source in an easy-to-understand manner. However, this will still require the public to want to know the quality and source of their information."

Carol Chetkovich, professor emerita of public policy at Mills College, commented, "My negative assessment of the information environment has to do primarily with my sense that consumers of media (the public at large) are not sufficiently motivated and well-enough educated to think critically about what they read. There will always be some garbage put out by certain sources, so, although it's important that garbage be countered by good journalism, without an educated public, the task of countering fake news will be impossible."

Peter and Trudy Johnson-Lenz, founders of Awakening Technology, combined on this response: "If we rely on technological solutions to verify trust and reliability of facts, then the number of states of the control mechanisms must be greater or equal to the number of states being controlled. With bots and trolls and all sorts of disinformation, that's virtually impossible. There are probably some tech solutions, but that won't solve the entire problem. And walling off some sections of the information ecosystem as 'trusted' or 'verified fact-filled' defeats the purpose of open communication. … If you study microtargeting during the 2016 election, it's clear that Facebook in particular was used to spread disinformation and propaganda in a very effective manner. This kind of activity is hard to discern and uncover in real time, it adds greatly to the polluted ecosystem and it is virtually impossible to control. Ultimately, people are going to have to make critical-thinking discernments themselves. Unfortunately, there are people who have no interest in doing that, and in fact discourage anyone else from doing that. The echo chamber is noisy and chaotic and full of lies. The only hope is some combination of technological advances to trust and verify, people being willing to take the time to listen, learn and think critically, and a rebuilding of trust. In our accelerating world, that's a very big ask! For an eye-opening perspective on acceleration, see Peter Russell's recent essay, 'Blind Spot: The Unforeseen End of Accelerating Change.'"

Bruce Edmonds, a respondent who shared no additional identifying details, said, "Lack of trust and misinformation are social problems that will not be solved with technical or central fixes. Rather, political and new normative standards will need to be developed in society."

Anonymous respondents wrote:
- "Bad information has always been produced and promulgated. The challenge remains for individuals to stay skeptical, consider numerous sources and consider their biases."
- "The way to solve the issue is not so much in designing systems for detecting and eliminating fake news but rather in educating people to manage information appropriately. Media and information literacy is the answer."
- "Continued misinformation will help people to learn first-hand how bad information functions in any system."

Responses to five additional follow-up questions regarding the future of the information environment

This section includes a selection of credited responses to five follow-up questions made by many of the top analysts who participated in this canvassing.

You can find *complete* sets of all of the for-credit and anonymous responses to these questions online here:

- http://www.elon.edu/e-web/imagining/surveys/2017_survey/future_of_information_environment_anon.xhtml
- http://www.elon.edu/e-web/imagining/surveys/2017_survey/future_of_information_environment_credit.xhtml

Follow-up #1:
Is there a way to create reliable, trusted, unhackable verification systems? If not, why not? And, if so, what might they look like?

An overwhelming majority of respondents who answered this question said, "No." Many say it is worth the effort to try to create verification systems because they may be at least partially helpful. Most say it's impossible to have *commonly accepted,* "trusted" systems; some say widespread trust cannot be inspired in any system. Most say there can be no "unhackable" largescale systems. Many question the ability of systems to parse facts from fiction or identify accurately and in a widely accepted manner the veracity of information sources.

John Klensin, longtime leader with the Internet Engineering Task Force and Internet Hall of Fame member, commented, "'Reliable' implies a frame or reference or official version, 'trusted' is in the mind of the beholder, and 'unhackable' implies this is a technical problem, not a social one, but it has always been a social one in every regard other than, maybe, some identification and authentication issues."

Helen Holder, distinguished technologist for HP, said, "First, nothing is 'unhackable.' Second, higher reliability of information can be achieved with human and electronic validation of facts, using methods that traditional investigators and journalists are trained to do. Some of those techniques may be enhanced with machine learning to identify common indicators of false information. Third, gaining trust is much harder and requires a long track record of virtually perfect execution. Any failures will be used to discredit such a system. For example, the modern widespread distrust of the reliability of information from major media outlets, despite being reliable the vast majority of time, indicates that even low error rates will add to perception that there are no objective, reliable sources of information. Rapid corrections when new information becomes available will be essential so that no outdated content can be referenced."

Glenn Edens, CTO for Technology Reserve at Xerox/PARC, wrote, "Maybe, but it is not clear what an acceptable technology might be. Consumers of information need to take an active role in determining the quality and reliability of information they receive. This can happen via verifiable and trusted sources through subscriptions, certificates and verifiable secure protocols, of course this does not solve the problem of the 'commons' – the free marketplace."

Liam Quin, an information specialist with the World Wide Web Consortium (W3C), said, "We're working on [these issues] at W3C, but the boundary between the physical and virtual worlds remains a difficulty."

Is it possible to create such a system?
Some say probably not

Alejandro Pisanty, a professor at UNAM, the National University of Mexico, and longtime internet policy leader, observed, "No, only partial approximations serving specific outlooks are possible. Malicious intent will never go away and will continue to find ways against defenses, especially automated ones; and the increasing complexity of our environments will continue to be way above our ability to keep people educated."

Frank Kaufmann, founder and director of several international projects for peace activism and media and information, commented, "No it will not be possible. This is the wrong approach to fixing the 'news' problem. I call this the 'cops and robbers' approach."

John Wilbanks, chief commons officer, Sage Bionetworks, replied, "No. Because the weakness of all technical systems is the people involved – the designers, builders, and users.

And we're always going to be hackable. Until we get better (or die off and are replaced by people better able to deal with it) it won't improve."

Tim Bray, senior principal technologist for Amazon.com, observed, "I doubt it; people trust people, not systems."

Howard Rheingold, pioneer researcher of virtual communities, longtime professor and author of "Net Smart: How to Thrive Online," commented, "Because it is an arms race with the purveyors of untrustworthy information backed by both state actors and amateurs, I don't think it is likely that 100% reliable systems will last for long. However, a combination of education – teaching people how to critically examine online info and use credibility tools, starting with elementary school children, can augment technical efforts."

Bob Frankston, internet pioneer and software innovator, said, "No, because the world is inherently ambiguous. If anything, the wish for such a system feeds into an authoritarian dystopia."

Garth Graham, an advocate for community-owned broadband with Telecommunities Canada, explained, "We can only verify the source, never the information. The question assumes external authority and there is no external authority."

A **professor and researcher based in North America** commented, "It is not possible to create a reliable, trusted, unhackable verification system. Trust is a social value that must be developed and maintained over time. The system will be only as trusted as the institution responsible for its maintenance. I do believe that it is possible to maintain reliable and trusted systems, but it is not a technology problem. It is a problem of ongoing support, labor and social integration."

Andrew Odlyzko, professor of math and former head of the University of Minnesota's Supercomputing Institute, observed, "No, because what is accepted as reliable is a social construct, and in most cases does not have an absolute, unambiguous answer."

Wendy Seltzer, strategy lead and counsel for the World Wide Web Consortium, replied, "No. We should focus on ways to reduce the impact and reach of falsehoods and spoofs, because we won't be able to stop them entirely. In a combined social-technical system, technical solutions aren't enough."

Mark P. Hahn, a chief technology officer, wrote, "No. Even with perfect tools people will make mistakes. Decentralized tools will still allow bad actors to subvert locally. Centralized tools will concentrate power and become both a target and a magnet for bad actors on the inside."

Matt Stempeck, a director of civic technology, noted, "Most verification signals can be misappropriated by third parties, as we've seen in the recent spates of sophisticated phishing attacks. More problematic is that many information consumers judge the content based on the person they know that's sharing it, not a third-party verification system."

An **anonymous respondent** replied, "No, because humans will go on getting information from all sorts of sources, some of which are less reliable than they think."

An anonymous **software engineer based in Europe** said, "It's going to be painful. People will continue to discard anything that doesn't fit in their bubble as 'untruth,' and dispute the verification."

An anonymous **North American research scientist** said, "We can't force the purveyors of misinformation to forgo their profits. Traditional news organizations have less authority and power, especially among those who only believe the purveyors of misinformation. The government cannot limit speech. Who will?"

Such a system would be too costly and work-intensive

An **executive consultant based in North America** echoed the voice of a number of other respondents when he said, "Yes, there are ways, but it is difficult and costly. Therefore, no one is motivated to do it. Right now, there are tech tools and algorithms that can point to suspicious sources of bad information, but it will take human intervention to step in, identify items and the source, and make the decision to intervene. That will be costly."

An **associate professor** said, "There may be but doing so would require a lot of capital. The question is then where would the financial and technical resources come from, and what are the motives of those providing them?"

A **participant in the projects of Harvard's Berkman Klein Center for Internet & Society**, said, "They will be complex and unwieldy, similar to high-level security, and in the

same way, will be largely ignored or misused by all but the most sophisticated consumers. Effective systems will require mutli-factor verification, third parties and watermarking."

There is likely to be less profit if such systems are implemented

Several respondents said there's too much money at stake to really put a stake in fake news.

Giacomo Mazzone, head of institutional relations for the World Broadcasting Union, replied, "I'm afraid there will be no way because the fundamental economic model will not change."

Justin Reich, assistant professor of comparative media studies, MIT, noted, "The better question is 'Will Facebook create a reliable verification system?' since that platform has achieved unprecedented status as the dominant source of news for Americans. They won't develop such a system because it's antithetical to their incentives and technically infeasible. Fake news is the kind of high-throughput, viral content that's terrific to sell ads against. Moreover communities really enjoy shared fake news: Judith Donath has important research here suggesting that sharing fake news can provide powerful signals of group affiliation even when people know it's fake. Spreading fake news is a mechanism for self-expression and for building community building – both squarely within the mission of Facebook. It's also financially lucrative to allow, and politically very difficult to deal with, since the bulk of Fake News comes from the Right and they are in political ascendancy. The corrosive effects of fake news on our society are but an unfortunate externality. Compounding the problems with incentives, algorithms can be reverse engineered and gamed, and crowd-sourcing methods will lead to mobilizing ideological crowds versus mobilizing people committed to objective truths. Fake news verification systems need to be built inside people's heads."

An **institute director and university professor** said, "Google, Facebook, Twitter and the like know there's no money in reliable, trusted, unhackable verification systems... Telling people what they want to hear, no matter for the truth, will always be more profitable."

An **internet pioneer and principal architect in computing science** replied, "If advertisers sign a pledge not to allow their ad money to flow to unreliable untrusted sources, then there will be an incentive to change – and with incentive, technical measures can be implemented."

Jerry Michalski, futurist and founder of REX, replied, "If Mark Zuckerberg wanted to play watchdog, he could turn Facebook, one of the superconductors of unreliable info, into a far better platform. But he'd risk growth and loyalty. A novel platform that is very reliable will have trouble attracting users, unless it is the natural successor to Facebook, Instagram, Snapchat, et cetera."

Is it possible to have *commonly accepted*, 'trusted' systems? It's complicated. 'What I trust and what you trust may be very different'

Paul N. Edwards, fellow in International Security, Stanford University, commented, " Any trusted verification system will require a significant component of attention from trained, reliable, trustworthy human beings. Such systems are labor-intensive and therefore expensive. Further, many people care more about confirming their own biases than about finding trustworthy sources."

A **research scientist based in North America** commented, "Who will be the referee?"

An anonymous **research scientist** replied, "'Verified' statements would simply be those in agreement with the ideology of the verifier."

Jamais Cascio, distinguished fellow at the Institute for the Future, noted, "Unhackable? No. Whether it's a technological hack or social engineering, we have to operate as if 'unhackable' is un-possible. Reliable? Probably. Trusted? Now this is the problem. Trust is a cultural construct (as in, you trust when the source doesn't violate your norms, put simply). What I trust and what you trust may be very different, and finding something that we both (or all) will trust may be functionally impossible. No matter the power of the technologies, there's still the 'analog hole' – the fact that the human mind has to accept something as reliable and true."

Daniel Kreiss, associate professor of communication, University of North Carolina-Chapel Hill, commented, "I doubt that a polarized public where partisanship is akin to religious identification will care about verified information. Members of the public would care about these systems if the information they parlayed benefits their own partisan team or social identity groups."

Edward Kozel, an entrepreneur and investor, replied, "All existing or posited techniques to grade 'trust' are subjective. Like reputation, trust is relative and subjective."

danah boyd, principal researcher, Microsoft Research, and founder, Data & Society, wrote, "Nothing is unhackable. You also can't produce trust in a system without having trust in the underlying incentives and social infrastructure. If you want to improve the current ecosystem, it starts by addressing perceptions of inequality."

Esther Dyson, a former journalist and founding chair at ICANN, now a technology entrepreneur, nonprofit founder and philanthropist, expert, said, "The systems can be unhackable, but they cannot be reliable and trusted any more than *people* can be reliable and trusted."

Leah Lievrouw, professor in the department of information studies at the University of California-Los Angeles, observed, "There may be some useful techniques for verification, but historically there's always been a dynamic in digital technology development where different parties with different views about who or what that technology is for, build and reconfigure systems in a kind of adversarial or 'argumentative' cycle of point-counterpoint. That's the culture of computing; it resists stabilization (at least so far). For me, though, the key thing is that verification isn't judgment. Fact checking isn't editing or making a case. It takes people to do these things and the idea that machines or 'an artificial intelligence' is going to do this for us is, I think, irresponsible."

An **anonymous respondent** wrote, "No, the verification system has to have an opinion."

Daniel Wendel, a research associate at MIT, said, "The technology exists to make things reliable and unhackable. However, this does not mean they will be reliable or trusted. At some level, value judgments will be made, and person preference will be injected into any system that endeavors to report on 'truth.' Luckily, having a fully foolproof, trusted and reliable source is not required. In fact, having a public that doubts everything is good. That said, some sources are more reliable than others. People need to begin to understand that being a wary consumer does not mean taking all news as 'equally fake.' There is a certain willful self-deception in society now that allows untruthful sources to be perceived as reliable. But social, not technical, innovation is required to overcome that."

Seth Finkelstein, consulting programmer with Seth Finkelstein Consulting, commented, "The technical issue of verification is irrelevant to the social issue of not valuing truth. That is, a cryptographically signed statement does almost nothing against being quoted in misleading manner, or just plain lies that people want to believe. The problem with stories 'too good to check' isn't a deficiency of ability, but rather essentially nobody cares. In discussion forums, when someone posts an article link and mischaracterizes it in an

inflammatory way, consider how few people will read the full article versus immediately ranting based on the mischaracterization. That is, we see a prominent failure-mode of not verifying by reading an article often one click away. Given this, it's hard to see more than a minuscule effect for anything elaborate in terms of an unforgeable chain to a source. It's worthwhile to compare the infrastructure of online shopping, where a huge amount of money is directly at risk if the system allows for false information by bad actors, i.e. credit card scammers. There, the businesses involved have a very strong incentive to make sure all the various platforms cooperate to maintain high standards. This isn't an argument to treat getting news like making a purchase. But looking at the overall architecture of a payment system can shed some light on what's involved in having reliability and trust in the face of distributed threat."

A **consultant based in North America** wrote, "Adoption of verification systems will be strongest among those who seek them out, a demographic that is not at the center of the political disinformation problem. Further, the intervention of verification could well serve (in the short term) to deepen the dogmatic lines of ideological division."

Scott Guthrey, publisher for Docent Press, said, "Ultimately the security will depend upon the humans building and using the system. There is no such thing as a 'reliable, trusted, unhackable' human being."

David Weinberger, writer and senior researcher at Harvard's Berkman Klein Center for Internet & Society, said, "Reliability and trust are social formations: Reliable and trustworthy enough for some purpose. We will adjust our idea of what is an appropriate degree of reliability and trust. Because we have to."

Can systems parse 'facts' from 'fiction' or identify accurately and in a widely accepted manner the veracity of information sources?

A **professor of law at a major U.S. state university** commented, "I don't think this is a technological problem. We had reliable, trusted verification systems. It was called journalism. But journalism stopped being a profession and became an industry. And accuracy was not advantageous to the bottom line. We need to rebuild not-for-profit media and help it cut through the online and cable clutter."

Eileen Rudden, co-founder of LearnLaunch, wrote, "We will be able to verify who you are, but will not be able to verify if what you say is true."

Erhardt Graeff, a sociologist doing research on technology and civic engagement at the MIT Media Lab, said, "Solutions to misinformation will be more social than technical and will require we redistribute power in meaningful ways. Using the frame of security, there is never going to be such a thing as an unhackable verification system. The weakest links in security are human, which cannot be addressed by technical fixes. Rather, they require that we work on education and support systems, designs that are collaboratively created and adaptive to people's needs, and ways to respond to hacks and crises that protect and reassure individual users first rather than business interests. Furthermore, conspiracy theorists will always find a way to discredit a system's reliability and trustworthiness. A more fundamental solution will require that we work on building relationships among diverse communities that foster mutual respect and trust. These networks of people and institutions are what information ecosystems (and democracies, more generally) work through. It's these webs of relationships that do the lion's share of the work of verification. We will need to rethink our connections to public information in order to foster respect and trust through consistent engagement in the same way friendships are built. News organizations, platforms, and other media elites will need to operate in more 'localized' and participatory ways that allow regular people to have agency in the journalistic process and in how problems like misinformation are addressed. We trust who and what we know in part because we have some control over those relationships closest to us. Ultimately, verification and the larger universe of information problems affecting democracy boil down to relationships and power, which we must take into account in order to make real progress."

Geoff Scott, CEO of Hackerati, commented, "Reliable and trusted in whose eyes? It's technically feasible to create immutable and consensus-based repositories for information, but it is the 'facts' themselves that are being doubted and fabricated. What determines if a statement is true or not? Popular consensus only indicates which statements are most believable to a segment of the population. Findings from 'independent' investigations are themselves questioned by those who are already inclined to disagree."

A **professor at MIT** commented, "'Slow' news, with adequate research and sourcing, still offers established venues credibility. It will take real forensic effort to keep up with technological fakery (lip-syncing unspoken words, compositing unlived images, generating chaff by bot-driven social media). We need to include the education of media-literate citizens in our fix, and to do that as a priority. The down side of 'fact control' (as opposed to critical thinking) is its ease of misuse."

Michael Zimmer, associate professor and privacy and information ethics scholar, University of Wisconsin-Milwaukee commented, "Any attempt at a system to 'verify'

knowledge will be subject to systemic biases. This has been the case since the first dictionary, the evolution of encyclopedias from a roomful of editors to a million contributors, debates over standardized curriculum, et cetera. Technology might make things appear to be reliable or unhackable, but that's just a facade that obscures latent biases in how such systems might be built, supported and verified."

Philipp Müller, postdoctoral researcher at the University of Mainz, Germany, replied, "I am skeptical that verification systems can be reliable and trustworthy if their decision is a binary one between true or false. In many instances, truth is a social construction. The ultimately trustworthy answer to many questions would therefore be that there is no ultimate answer but rather different sides to a coin. I believe this logic of uncertainness and differentiated 'truths' is hard to implement in technological ecosystems."

Alfred Hermida, associate professor and journalist, commented, "The question assumes there is an objective 'truth' that can be achieved. Who and how information is verified is shaped by systemic power structures that tend to privilege sectors of society."

Rick Forno, senior lecturer in computer science and electrical engineering at the University of Maryland-Baltimore County, said, "There is no unhackable system for facts or the presentation of reality; people will still believe what they want to believe. Technology can help increase the level of trust and factual information in the world, but ultimately it comes down to the individual to determine what is real, true, fake, misleading, mis-sourced, or flat-out incorrect. That determination is based on the individual's own critical-thinking skills if not the factual and practical soundness of their educational background as well. Unfortunately, I don't see technology helping overcome *that* particular vulnerability which is quite prevalent in the world – i.e., people making bad judgments on what to believe or trust – anytime soon. I hope your report's commentary will touch on the importance of not only education (both formal and informal) and especially the development of critical-thinking and analysis skills needed to inculcate an informed and capable citizenry – especially ones that allow a person to acknowledge an opposing view even if they disagree with it, and not just brush it off as 'fake news' because they don't like what they're hearing or seeing. Otherwise, I daresay a misinformed or easily-misguided citizenry that remains uncritical and unquestioning will remain a politician's best friend, and this problem will only get worse in time. ;("

There can be no unhackable largescale networked systems

Michael R. Nelson, public policy executive with Cloudflare, replied, "No one who works on computer systems would promise that a system can be 'unhackable.' But a lot can be done with a system that is 'good enough' and upgradable (if vulnerabilities are found). The history of encryption is a good model. Standards have evolved to overcome new attacks."

A **leading internet pioneer** who has worked with the FCC, ITU, GE, Sprint and VeriSign commented, "This cannot be done with an open TCP/IP internet."

David Conrad, a chief technology officer, replied, "No, not systems that can be deployed in a cost-effective fashion for the foreseeable future. 'Unhackable' implies a fundamental change in how computer systems and software are implemented and used and this is both expensive and takes time."

A **professor of law at a major California university** noted, "Reasonably reliable and trusted, yes. Completely unhackable? We have not managed it yet, and it seems unlikely until we can invent a system that, for example, has no vulnerabilities to social engineering. While we should always work to improve reliability, trust and security on the front end, we must always expect systems to fail, and plan for that failure."

Timothy Herbst, senior vice president of ICF International, said, "I don't think there will ever be an 'unhackable verification system,' and it would be folly to believe in such a thing."

Brad Templeton, chair emeritus of the Electronic Frontier Foundation, said, "Reliable and trustable, but not unhackable. However, the level of intrusion can be low enough for people to use them."

It's worth it to create verification systems; they may work somewhat or at least be helpful

Jonathan Brewer, consulting engineer for Telco2, commented, "Yes, it's very possible to create trusted, un-hackable verification systems. Much of the requisite infrastructure exists through DNSSEC. Browser vendors and social media platforms need only integrate and extend DNSSEC to provide a registry of authentic information sources."

Micah Altman, director of research for the Program on Information Science at MIT, commented, "People and the systems they create are always imperfect. Instead of 'unhackable' systems we should seek more reliable, more trustworthy and tamper-resistant (hardened) systems. These systems will be based on transparency of operation (e.g., open source, open algorithms); cryptographic protocols; and distributed operation."

A **senior fellow at a center focusing on democracy and the rule of law** commented, "Full reliability is not attainable. But there already exist general principles that can be used to reduce the spread of false information. Examples include: penalizing the organizations (newspapers, Facebook pages, Twitter accounts) that spread malicious information (e.g., libel laws); make trolling a punishable offense (e.g., hate speech); mechanically block distributors of malicious information (e.g., censorship – note that this particular approach can also be used to block the circulation of reliable information by non-democracies/non-democrats); encourage ethical reporting (e.g., insist on at least two independent direct sources as evidence)."

A **professor at a major U.S. state university** said, "Yes. A lot can be accomplished with: **1)** Automated analysis of the text, **2)** Automated analysis of the sources, and **3)** Social processes to suppress fake news."

Susan Hares, a pioneer with the NSFNet and longtime internet engineering strategist, now a consultant, said, "Yes, reliable, trusted unhackable verification systems are within the range of today's technology. The public writers and readers can be protected by current cryptography algorithms if new methods for storing and retrieving public information are created. As public outcry increases for fake news, then the requirements to have multiple sources document and tested within a program can be done. Academic systems already do cross checking of academic sources. The real problem today is that it costs to secure these systems. If the citizens of United States or other countries want these systems, then the public and private money must be invested to create them."

Filippo Menczer, professor of informatics and computing, Indiana University, wrote, "Yes. We can develop community trust standards backed by independent news and fact-checking organizations, and implemented by Web and social media platforms. It won't be perfect and abuse will continue to exist, but its harm will be reduced."

Irene Wu, adjunct professor of communications, culture and technology, Georgetown University, said, "There is no perfectly unhackable system. If there were, they could be used for harm as easily as for good. However, we may develop technical ways to improve the

quality of news we get. In other arenas, we rely on safety certifications for home appliances, or brand names for fashion clothing. Similarly, other markers could be developed for information. It used to be we trusted a newspaper, maybe it's no longer just the newspaper, but a certification that reporters can get, or an industry association of online news sources that adheres to good codes of practice."

Steve McDowell, professor of communication and information at Florida State University, replied, "A reference system (a trusted source vouches for the author or story in question) or a branded system (recognizable and trusted information providers) may reduce to persuasivenes of some false facts. However, there may not be agreement on who are the trusted sources in [the category of] news and information."

Michael Wollowski, associate professor at the Rose-Hulman Institute of Technology, suggested there is trusted news, writing, "It's called the New York Times [for facts]. We always had the National Enquirer [for fake news]. It is just that now we have many more information sources. If you want to read them, go ahead. If you want to trust information, do what people have been doing for a long time: peruse sources that are known to diligently check their facts. Use sources from several countries/continents."

Bart Knijnenburg, researcher on decision-making and recommender systems and assistant professor of computer science at Clemson University, said, "A lot depends on (automated) social proof. Algorithms will learn to filter out 'bad apples.' This is crucially dependent on having the right incentives: the appeal of 'virality' will go away once news consumption is no longer funded by ad consumption."

A **research scientist based in Europe** said, "Ask legitimate news sites to be more thorough in the way they report information, because recently the quality of the content of major media (e.g., CNN, Fox News, NY Times) has been declining."

Larry Diamond, senior fellow at the Hoover Institution and FSI, Stanford University, wrote, "I won't comment on the technical dimensions, but I do think we can get more reliable and trusted information if the digital platforms invest greater human and technical resources in vetting and verification. I definitely don't want to see governments play this role."

An anonymous **CEO and consultant based in North America** suggested a solution: "Create and use smaller autonomous networks where peering is based solely upon trust."

A **principal network architect** said, "The process already exists. It is called earning the respect of one's peers. It can't be perfect but it works most of the time."

An **anonymous respondent** replied, "There can still be a place for professional journalists who really investigate and earn public trust. Plus there are our peers around us, but with them our trust may be misplaced sometimes."

Marc Rotenberg, president, Electronic Privacy Information Center, wrote, "Yes, but it will require a much greater willingness in the U.S. to pursue antitrust investigations and to support the enactment of data-protection laws."

Rob Atkinson, president, Information Technology and Innovation Foundation, said, "If nations copied Estonia's digital signature model we could have trusted verification systems. These would bring an array of other economic benefits as well."

Larry Keeley, founder of innovation consultancy Doblin, commented, "YES. I've had teams working on in both the design school where I teach graduate and doctorate students, plus at the Kellogg Graduate School of Management. There are technologies – like blockchain and other forms of distributed ledgers – that make complex information unhackable. There will be other methods that don't worry so much about being unhackable, and worry more about being resilient and swiftly corrected. There will be many more such emergent capabilities. Most, however, will NOT be instantaneous and real-time, so that there will still be considerable asymmetry with information that is compelling, vivid, easily amplified, and untrue. So the coolest systems may need to have an augmented-reality 'layer' that provides the confidence interval about the underlying story – and shows how that gets steadily better after a bit of time permits a series of corrective/evaluative capabilities to address the initial story(ies)."

Henning Schulzrinne, professor and chief technology officer for Columbia University, said, "We only need near-perfect, not perfect, systems. Verification systems within limited realms are feasible, both for identifying publishers and individuals."

Sonia Livingstone, professor of social psychology, London School of Economics and Political Science, replied, "…Reliable and trusted systems – as we already have with banking, for instance – are possible and likely. There's probably, in the end, more money and power to be gained by building systems the majority trust than in creating widespread distrust and, ultimately, a withdrawal from the internet (or, even, some as-yet hard-to-imagine alternative system being built)."

Riel Miller, an international civil servant who works as team leader in futures literacy for UNESCO, commented, "Reliable, trustworthy and secure 'verification systems' are in the eye of the beholder and context. A 'truth' vending machine or system is not doable. What is entirely feasible and is always more or less functional are systems for assessing information in context and related to need. With the decline in the status and power of the former gatekeepers of 'good' knowledge processes are unleashed to seek alternatives. Mass solutions are not the only way and are likely to be sub-optimal from many perspectives. As new sources and dynamics for counter-vailing power emerge so too will fit for purpose assessment. It will be messy and experimental, that's complex evolution."

The **president of a business** wrote, "Nothing is ever unhackable. But social engineering, editors, educational systems, the Wikipedia-style hive mind solution, and judicious law-making, combined with the type of AI that identifies fraud on a credit card, can make great strides toward protecting information systems and news."

Paul Gardner-Stephen, senior lecturer, College of Science & Engineering, Flinders University, disagreed with Livingstone and the other optimists, writing, "One of the problems is that it is state-level actors who are major players in this space. Tools like blockchains may allow for consensus forming and similar web-of-trust schemes, however they all stumble over the problems of relativity, subjectivity and perspective. We see this today: One man's bullying is another's 'standing up for himself.' This is a classic tragedy of the commons: The rules that enabled public communications to be productively shared are being undermined by those so desperate to hold onto power, that they are willing to degrade the forward-value of the medium. Indeed, for some, it is probably an active ploy so as to neuter public scrutiny in the future by destroying and discrediting the means by which it could occur."

'Verification' would reduce anonymity, hinder free speech, harm discourse

Most respondents said requiring user verification systems would be likely to require the loss of anonymity and the appointment of an overall authority, which could limit online participation and free expression for many people.

John Perrino, senior communications associate at George Washington University School of Media and Public Affairs, wrote, "You would either put First Amendment rights at risk by only allowing verified content from a few sources or expand the verification system to everyone where it is sure to be exploited because it would be created by humans."

A **senior policy researcher with an American nonprofit global policy think tank** said, "Verification starts with the reduction of anonymity." A **professor and researcher of American public affairs at a major university** replied, "No, such a system is unlikely, at least not without creating unacceptable limits on who can express themselves online." A **media director and longtime journalist** said, "There is no absolute trust without an end to anonymity. Even then, human trust is hackable using economic/social/moral/peer pressure."

Nathaniel Borenstein, chief scientist at Mimecast, commented, "No [such system is possible]. Not without an absolute authority that everyone is required to trust."

An anonymous **research scientist** said, "I am not aware of any such system in the history of mankind. In fact, any system that actually *did* what you describe would probably be regarded as the instrument of an oppressive regime. For me, contestation, explanation, agonism are what a healthy information ecosystem is about – and not one that outsources accountability to 'verification systems.'"

An **anonymous respondent from the Berkman Klein Center at Harvard University** noted, "No. A 'reliable' and 'unhackable' verification system implies policing the information we share and how we share it. That would seem to stand in opposition to a free exchange of ideas, however stupid some of those ideas might be. But placing the responsibility for assessing the quality of information on the listener keeps the channels open. Unfortunately, it's far from foolproof. And there's no reliable way to train people to be better, more critical listeners or consumers of information."

Some hopeful proposals for possible fixes and deeper looks at the issue

Peter Jones, associate professor in strategic foresight and innovation at OCAD University, Toronto, predicted, "The future will look like a network of commentary and field-level ('embodied') tweets supported by well-funded Wikileaks sources that cue journalists and give direction to investigation. Wikileaks is not 'hackable' in the way today's fake news attributes such 'hacks' to Russia. False information on a leak site is crowd-analyzed and found out quickly."

Amy Webb, author and founder of the Future Today Institute, suggested solutions, writing, "There is a way to create reliable, trusted verification systems for news, but it would require radical transparency, a fundamental change in business models and global cooperation. Fake

news is a bigger and more complicated problem than most of us realize. In the very near future, humanity's goal should be to build international, nonpartisan verification body for credible information sources. Within the decade, machine learning can be applied for auditing - randomly selecting stories to fact-check and analyze expert sentiment. In the decade that follows, more advanced systems would need to authenticate videos of leaders as real, monitor augmented reality overlays for hacks, ensure that our mixed reality environments represent facts accurately. The best defense against fake news is a strong, coordinated offense. But it will take cooperation by both the distributors – Facebook, Google, YouTube, Twitter – and the world's news media organizations. Google and Facebook could take a far more aggressive approach to identifying false or intentionally misleading content and demoting websites, channels and users who create and promote fake news. Twitter's troll problem could be tackled using variables that analyze tweet language, hashtag timing, and the origin of links. YouTube could use filters to demote videos with misleading information. News organizations could offer a nutritional label alongside every single story published, which would list all the ingredients: everyone in the newsroom who worked on the story, all of the data sets used, the sources used, the algorithms used, any software that was used, and the like. Each story that travels digitally would have a snippet of code and a badge visible to viewers. Political stories that are factually accurate but represent liberal or conservative viewpoints would have a verification badge indicating a political slant, while non-political stories would carry a different badge. The easiest way to do this would be to use the existing emoji character system. The verification badge convention is something we're already familiar with because of Twitter and Facebook. Similarly, stories with verified badges would be weighted more heavily in content distribution algorithms, so they would be prioritized in search and social media. Badges would be awarded based on credible, factual reporting, and that wouldn't be limited to traditional news organizations. Of course, it's possible to hack anything and everything, so whatever system gets built won't be impenetrable."

Jonathan Grudin, principal design researcher, Microsoft, said, "Verifying the accuracy of information claims is not always possible, but verifying the source of information seems likely to be tractable. The next step is to build and learn to use reliable sources of information about information sources. This can be done now most of the time, which isn't to say unforeseen technical challenges won't arise."

Marcel Bullinga, futurist with Futurecheck, based in the Netherlands, said, "I envision an AI-backed, traffic light system that shows me in realtime: Is this information/this person/this party reliable, yes or no? Is their AI transparent and open, yes or no? Is their way of being financed transparent, yes or no?"

A **senior researcher and distinguished fellow for a major futures consultancy** observed, "In the long term, very sophisticated multi-factor biometrics may mitigate risks at the human end. Meanwhile, advanced interconnected secure blockchain fabrics, may extend considerable security to future microservices, Internet of Things automation and valuable data and media."

The **chief technology strategist for a nonprofit research network serving community institutions**, commented, "We may see a combination of Wikipedia-like curation combined with blockchain for determining provenance."

Diana Ascher, information scholar at the University of California-Los Angeles, said, "I suspect many will advocate for the use of artificial intelligence to build trustworthy verification systems. However, always inherent in such systems are the biases and perspectives of their creators. The solution to biased information must come in the form of a recognition on the part of the information seeker that no information is pure fact. It is all interpreted and deployed in context. Systems that present information from a variety of perspectives will be most effective in providing the public with the opportunity to understand the many facets of an issue. And then, of course, most people will accept as true the information that confirms their existing beliefs. In addition, news consumers depend on heuristic information practices to find the information on which they base their decisions. Often, this comes in the form of opt-in communications from emerging thought leaders as trusted sources, as we're seeing in the resurgence of email digests from individuals and think tanks (e.g., Stat, Neiman, countless others), as well as following trusted entities on social media (e.g., Twitter)."

Judith Donath, fellow at Harvard's Berkman Klein Center, and founder of the Sociable Media Group at the MIT Media Lab, wrote a detailed reply:

"There's no single answer – there is and will continue to be a technological arms race, but many of the factors are political and social. Basically, there are two fronts to fighting fake news. The first is identifying it. This can be a technical issue (figuring out the ever more subtle indicators of doctored video, counterfeit documents), a research problem (finding the reliable documentation that backs a story), et cetera. The second, harder, one is making people care. Why have so many Americans embraced obvious lies and celebrated the liars? And what can we do to change this? Many feel a deep alienation from politics and power in general. If you don't think your opinion and input matters, why should it matter how educated you are on issues?

"Rethinking news and publishing in the age of the cellphone should not be just about getting the small screen layout right, or convincing people to <like> a story. It needs to also be about getting people to engage at a local level and understand how that connects with a bigger picture. An authoritarian leader with contempt for the press is, obviously, a great boon for fake news; an authoritarian leader who has the power to control the press and the internet is worse. Socially, the key element is demand for truth – the 'for-profit-only' writers of some of last fall's fake news had little interest in whether their stories were for the right or the left – but found that pro-Trump/anti-Hillary did well and brought them profits, and that there just wasn't the same appetite on the left.

"We need to address the demand for fake news – to motivate people across the political spectrum to want reality. This is not simply a matter of saying 'read critically, it is better for you' – that is the equivalent of countering a proselytizing Christian telling you to believe in the Gospels because Jesus walked on water by explaining the laws of physics. You may be factually right, but you won't get anywhere. We need to have leaders who appeal to authoritarian followers AND also promote a fact- and science-based view of the world, a healthy press ecology etc.

"That said, the technology – the internet, AI – has changed the dynamics of fake news. Many people now get their news as free floating stories, effectively detached from their source publication. So one issue is how to make news that is read online have more identity with the source, with the reasons why people should believe it or not. And the answers can't be easy fixes, because any cheap signal of source identity can be easily mimicked by look-alike sites.

"The real answer will come with finding ways to work WITH the culture of online reading and find native ways to establish reliability, rather than trying to make it behave like paper. A key area is the social use of news in a platform like Facebook. We've seen the negative side – people happy to post anything that they agree with, using news as the equivalent of a bumper sticker, not a source of real information. News and social platforms – both the publishers and the networks – should create tools that help people discuss difficult issues.

"At the moment, it appears that what Facebook might be doing is separating people – if they disagree politically, showing them less of each other's feeds. Instead, we need tools to help mediate engagement, tools that help people host discussions among their own friends less acrimoniously. Some discussions benefit from interfaces in which people up and downvote different responses; some interfaces present the best comments more prominently, etc. While not every social discussion on Facebook should have more structured interfaces and

moderation tools, giving people the ability to add structure etc. to certain discussions would be useful.

"I would like to see newspapers do a better job of using links to back up stories, provide background information and more detailed explanations. While there is some linking in articles today, it is often haphazard – links to Wikipedia articles about a mentioned country, etc. rather than useful background information or explanations or alternative views. The New York Times is doing a great job in adding interactive material – I'd like to see more that helps people see how different changes and rules and decisions affect them personally."

Barry Chudakov, founder and principal, Sertain Research and StreamFuzion Corp., wrote, "The way to ensure information is trustworthy is to build trust-tools into the information itself. By transparently revealing as much metadata and tracking confirmation of the sources of the information, readers and viewers can verify the information. This not only enhances the value of the information, it fosters confidence and reliability.

"Many useful organizations such as Check, an open web-based verification tool, FactCheck.org, PolitiFact, the International Fact-Checking Network at Poynter Institute, Share the Facts, Full Fact, Live – all are tackling ways to institute and evolve trusted verification systems. Fifteen years ago in 'Making the Page Think Like a Network,' http://bit.ly/2vyxQ3l, I proposed adding an *information balcony* to all published information; in this balcony, or level above the information itself, would appear meta-commentary about the utility and accuracy and of the information.

"With tracking tools and metadata – today mostly in the hands of marketers, but useful for the larger public good – we can verify messaging and sources more accurately than ever before because information now carries – within its digital confines – more miscellaneous data than ever before. A Facebook post, a tweet, notes from a meeting, an audio recording, contemporaneous notes from an anonymous source – all can be combined to create trusted, verifiable content that reveals any hacking or alteration of the content.

"With meta information positioned in a balcony above or around the information, readers and viewers will become accustomed to evaluating the reliability of the information they receive. We can no longer behave as though information can operate alone on *trust-me*. Just as RSA, the security division of EMC, provides security, risk and compliance management solutions for banks; media outlets will need to provide an added layer of information protection that is *a visible component of the information presentation itself*, whether online or in broadcast and print.

"Some countries are already doing this. As the *Washington Post* reported recently, 'When politicians use false talking points on talk shows that air on RAI, the public broadcast service in Italy, they get fact-checked on air. It's a recorded segment, and the hosts and politicians debate the data. Politicians frequently revise their talking points when confronted with the facts during interviews.' Work is already underway to enact better verification. A committee of fact-checkers, under the auspices of the International Fact-Checking Network developed a code of principles, to which The Washington Post Fact Checker was an inaugural signatory. Knowing that information is dynamic – that it can expand, deepen, change – is essential to creating reliable, trusted, unhackable verification systems."

Bernie Hogan, senior research fellow, University of Oxford, noted, "All systems must work on some web of trust. We live in post-modern times where we have long since departed from a world of absolute truths to one of stable regularities. Our world is replete with uncertainty. To make a system that is certain also makes it rigid and impractical. We already know that one-time pads form excellent unhackable security, but they are completely unrealistic in practice. So, I genuinely challenge the question – reliable does not mean perfect or unhackable. We must reject these absolutes in order to create more practical working systems and stop discourses that lend us to false equivalences between different paradigms. Some are still much more reliable than others even if they are not perfect."

An **author/editor/journalist** wrote, "If you view each piece of misinformation as a virus, trying to fight such a multitude of individual viruses is ridiculously difficult. Immunity from viral attack is the actual goal. That is only attained when the population gains high quality critical thinking skills. For those who missed out on this, the efficacy of such skills needs to be demonstrated by people with influence, frequently and explained well. In much the same way that it has become popular to look at parenting deficits through popular TV programs or even the detail of analysis which is invested in cooking programs. Without the popular uptake of critical thinking, misinformation will continue to be manufactured to appeal to specific subgroups by targeting their confirmation bias."

Alladi Venkatesh, professor at the University of California-Irvine, replied, "This is not easy, but we should not give up."

A selection of additional comments by anonymous respondents:
- "With cloud adoption up, there are more apps like academia.edu, experiment.com for information dissemination and crowd-funded science."
- "There is no complete solution, but nimbleness and adaptability will go a long way toward helping curb hacking and bad information."

- **"**The rapid development of the many-to-many communication system caught the world unprepared... The gatekeepers of the one-to-many communication systems (TV-press) are not valid anymore."
- "Trust should be based on reputation for sound reporting, not what garners the most clicks."
- "Changing the transparency model around systems to one where hacks and possible hacks are clearly defined by known interactions with specific systems at specific times is one possible path to resolving the trustworthiness of a source of information."
- "No. The problem is the lack of a clear categorical differentiation. There are two fuzzy dimensions, the extent of falsity and the motivation of the purveyor."
- "It is a matter of scale: if you want Facebook to do that for a billion users, it cannot happen since it is very hard to attend to minority views on a platform that wants to scale. On smaller scale, why not?"
- "Federated trust networks. At small enough scales they aren't worth the effort to hack."
- "Verification systems are only as good as their level of deployment."
- "The cost of hacking verification systems will continue to rise, but so will the rewards for doing so."
- "Wikipedia has demonstrated feasibility on open communities."
- "Platforms should deploy larger efforts to limit fake news and misinformation by white-listing reliable sources."
- **"**The biggest challenge is battling the narrative of mistrust, authoritarianism and racism."
- **"**Humans are the weak link in the chain, and they aren't getting any better."
- "What is to be verified, the source or the opinion?"
- "There is no universal truth and certainly no universal acceptance of 'facts.' It has ever been thus."
- "Analyzing other organizational systems like credit cards/banks may be a good idea to assess trust."
- "There is too much news content being shared in too many different places to ensure accuracy."
- "Security is about risk mitigation by reducing attack vectors, we can reduce the risk."
- "Anything that tries to tackle misinformation once it's already in the world will already be fighting a losing battle."
- "Construct something like the old 'Good Housekeeping Seal of Approval.'"
- "A successful solution would have to address people's desire to seek out the 'facts' they like rather than the truth."

- "The sources of news are so diffuse, and social networks so ingrained, that it may not be fully possible - is Facebook going to police the opinion of your Uncle Frank?"
- "This will never and should never be centralized. The internet welcomes all comers, so different homegrown verification systems will emerge."
- "Systems are not the answer. Norms and standards for discourse are the solution."

Follow-up #2:
What are the consequences for society as a whole if it is not possible to prevent the co-opting of public information by bad actors?

Most of the expert respondents in this canvassing said people have to adjust well and quickly to this new information environment or there could be extremely serious effects. Among their predictions are larger, seemingly insurmountable divides between social groups and the further fragmentation of society; people being overwhelmed by an avalanche of information in which they cannot discern fact from fiction; deepening distrust damaging the development of problem-solving policies; and the decline of democracy that results from an uninformed voting public and – possibly – a withdrawal by the public from civic engagement.

**Some worry we could be turning a corner into
an extremely dangerous time in human history**

An **internet pioneer and principal architect** in computing science replied, "Governments claiming to live in a 'post-truth' age slaughtered tens of millions during World War II, so we've seen the movie before. It didn't end well."

Jerry Michalski, futurist and founder of REX, replied, "My greatest fear at the moment is that the post-factual world isn't a three-year aberration but is instead a 300-year era, much like the 400 years after Gutenberg transformed and traumatized Europe."

A **professor of law at a major U.S. state university** commented, "America will look more and more like Russia. There will be more extremes of rich and poor, more corruption, more distrust."

A **project manager for the U.S. government** responded, "We will fight amongst ourselves and really do some serious damage to our way of life."

Joshua Hatch, president of the Online News Association, noted, "Honestly, I think it has the potential to lead to civil war. I don't think that will happen, but I do think those are the stakes."

A **research scientist for the Computer Science and Artificial Intelligence Laboratory at MIT** said, "In the most-extreme case, it could mean the dissolution of liberal democracies and replacement by chaos or tyranny. Any increase in risk of either should concern everyone, even if the probability is deemed small."

A **senior global policy analyst for an online citizen advocacy group** simply sent the link to a photo representing Dante's Inferno: https://media.npr.org/assets/artslife/arts/2010/02/dantesinferno/inferno_archive-becf91cdf5140a602f77b5514b518ba7db4db4f6.jpg?s=1400

Fredric Litto, professor emeritus, University of São Paulo, Brazil, wrote, "As a longtime student of information technology, I have long believed that a new 'sickness' would arise in modern society, one of increasing complexity in everyday life causing many people to resist leaving the security of their beds each morning, preferring to remain under the covers so as not to have to deal with decision-making and the exhausting need to constantly be learning new ways of working. If, in addition, we add to this situation the question of the insecurity arising from the inability – to never be able to entirely trust the information one encounters – there will inevitably be massive evidences of stress-provoked illness."

Stephen Bounds, information and knowledge management consultant, KnowQuestion, said, "This is the new reality of warfare today. Wars are going to be literally fought over 'information supply lines,' much as food supply lines were critical in wars of years gone by."

John Wilbanks, chief commons officer, Sage Bionetworks, replied, "We're there already. Polarized sub-groups refusing to acknowledge truth of anything they disagree with weaponized through intentional manipulation to lower trust in institutions and intermediaries. What's next is like this, but moreso."

Amber Case, research fellow at Harvard Berkman Klein Center for Internet & Society, replied, "The consequences for society are similar to what we've already seen: Greater rifts between political parties and social classes. Crime due to misunderstandings. A waste of advertising revenue on knee-jerk reactions instead of reflective ones. So much of our online meeting is about speed and reaction that we can't pause to take a breath before reacting."

Tom Valovic, Technoskeptic magazine, noted, "Consequences are discussed in my book 'Digital Mythologies': Postmodern chaos and moral relativism along the lines of exactly what we're seeing now."

David Wood, a UK-based futurist at Delta Wisdom, said, "We might blunder into World War III, a new Dark Age, or another existential disaster – driven there by foolish judgment and bad feelings stirred up by bad information."

Deirdre Williams, an internet activist, replied, "We will become a population of credulous slaves until the pendulum begins to swing in the opposite direction."

Mercy Mutemi, legislative advisor for the Kenya Private Sector Alliance, observed, "Manipulation. And not just during elections or referenda. I imagine a world in which simple policy decisions may be manipulated to the benefit of a few... Weaponized fake news could turn us all into robots and the worst part is we wouldn't even know we are being manipulated."

Michael Rogers, principal at the Practical Futurist, wrote, "False information is toxic for just about every level of decision-making, from personal (say, vaccination) to public (elections, say, or mobilizing a nation for war). Often one can't know information is toxic until it has been acted on, and then it's too late."

Morihiro Ogasahara, associate professor at Kansai University, said, "Democracies will be corrupt because of lack of credible information for decision making."

Charlie Firestone, executive director, Aspen Institute Communications and Society Program, commented, "The result is the road to authoritarian society where the people are left with the word and power of the state to give them the truth. Not a desirable state."

An **executive consultant** based in North America wrote, "The speed and broad spread of bad information could have devastating results – it has already impacted the outcome of a presidential election. It could also impact the markets and the economy by tainting corporate and personal reputations."

Esther Dyson, a former journalist and founding chair at ICANN, now a technology entrepreneur, nonprofit founder and philanthropist, expert, said, "The consequences would be increased cynicism and despair; general breakdown over the long term."

Howard Rheingold, pioneer researcher of virtual communities, longtime professor and author of "Net Smart: How to Thrive Online," said, "People will lose their liberties (we are already seeing that in the U.S.) because of political info-manipulation; people will lose their lives because of bad medical information."

Bob Frankston, internet pioneer and software innovator, said he hopes for the best, writing, "Faith may trump understanding. I think longer-term understanding will prevail because the ideas are more powerful. But it won't be a simple process of refinement."

Jamais Cascio, distinguished fellow at the Institute for the Future, noted, "Multiple scenarios are possible. We could see this as triggering a memetic immune system, where we develop both technological and cultural tools and methods to favor veracity over stimulation; we could see the further hardening of ideological barriers, with entire communities/regions becoming controlled in ways that bar wrong-think; we could see the disproportionate success of a particular worldview causing the followers of bad actors to fail. Two broad scenarios: **1)** civil conflict, where ideological and cultural divisions metastasize into violence; or **2)** our cognitive immune systems of skepticism and verification become stronger and society becomes healthier as a result."

An **anonymous internet pioneer and longtime leader in ICANN** said, "Consequences include wholesale fraud and other malicious behavior. We haven't been able to prevent it in real life, so why should we assume that we can do it in cyberspace?"

Democracy is damaged when people cannot trust in information; some are likely to be overwhelmed and simply give up on participating in civic life

Many respondents discussed the impacts of a misinformed, divided, confused populace on democracy, some of them noting how a lack of faith in a political system impacts every aspect of the life of a society.

Marc Rotenberg, president, Electronic Privacy Information Center, wrote, "The consequence is the diminishment of democratic institutions."

Thomas Frey, executive director and senior futurist at the DaVinci Institute, replied, "Failure to find a solution will mean rapidly deteriorating confidence in all systems including the stock market, financial systems and even voting/elections at the heart of a democratic society."

danah boyd, principal researcher, Microsoft Research and founder, Data & Society, wrote, "Democracies depend on functioning information ecosystems. If we don't address the fundamental issues at play, we could risk the collapse of democracies."

Evan Selinger, professor of philosophy, Rochester Institute of Technology, wrote, "A well-functioning democracy is inherently incompatible with a post-fact society. Full stop."

Ari Ezra Waldman, associate professor of law and New York Law School, wrote, "Democracy dies in a post-fact world. When the public square is so crowded and corroded by misinformation, misleading information, and outright lies, a number of things happen. First, trust falls. Trust in institutions, including the media, falls, spawning denialism and conspiracy theories. Second, knowledge falls. That is, society becomes less educated. When nothing is verifiable and everything is an opinion, people can start believing the Earth is flat and have no reason to doubt themselves because, as Mr. Trump has said about Russian hacking, 'no one really knows.' In a world where 'no one really knows' anything, anyone can say anything. Rationality, then, ceases to exist."

Dan Gillmor, professor at the Cronkite School of Journalism and Communication, Arizona State University, commented, "It would mean the end of democratic self-rule. If all information is equal, no matter whether it's true or false, benign or malign, we can't make decisions based on reality."

David Manz, a cybersecurity scientist, replied, "The result will be '1984': dystopian authoritarians and powers of all types can more easily manipulate the feelings of the people."

Charles Ess, a professor of media studies at the University of Oslo, wrote, "The consequences will be apocalyptic – at least for those of us who still believe in the basic notions of human freedom, sociability, rational discourse and affiliated rights to privacy and freedom of expression that ground democratic polity. The alternatives are already visible in Putin's Russia and elsewhere: societies masquerading as 'democratic' that are in fact thinly disguised electronic oligarchies that render most of us into feudal chattel."

Scott Shamp, an interim dean at Florida State University, commented, "We will be ruled by those who view accuracy as secondary to gaining advantage."

Rick Forno, senior lecturer in computer science and electrical engineering at the University of Maryland-Baltimore County, said, "The consequences are an uninformed, misinformed electorate that elects similar-minded people."

Serge Marelli, an IT professional who works on and with the Net, wrote, "The consequences are lots of Donald Trumps (or Putins, Erdogans, or…) in many countries."

Mike Meyer, chief information officer at University of Hawaii, wrote, "The current governmental and social structure will collapse."

A **professor of education policy** commented, "For some, it will mean the continued (or new) loss of the fundamental right to vote. For others, it will mean increasing precarity with fewer governmental safety nets to help cushion blows. For others it will mean loss of life, of property, of basic rights. For others, it will mean greater wealth, increased capacity to pillage natural resources, et cetera. And importantly, this is not U.S. society – this is global."

Jan Schaffer, executive director of J-Lab, said, "People will not be able to make informed choices, and will likely opt out of political participation. Bad actors will continue to be elected. Progress will be hampered by drama and a focus on maintaining power. Civil society will decline."

Uta Russmann, a professor whose research is concentrated on political communication via digital methods, noted, "Society as a whole will increasingly rely on software such as IBM Watson. Moreover, even though probably not in the next 10 years but in the long run, computers will become more intelligent than humans. In the next 10 years, around the world, almost everyone will have a smartphone and hence almost the same access to information and education. But this development will cause less trust between people."

A **professor of rhetoric and communication** wrote, "Our democracy depends on the presumption of shared facts, rational behaviors, and a kind of regularity and trust in the laws. Online, all information, even bald-faced lies, can be made to look equal to the actual facts. The consequences are that we swing from one extreme to another, that people stop talking to anyone they disagree with, that we move away from building trust based on a common set of values and truths."

Adam Gismondi, a researcher at the Institute for Democracy & Higher Education, Tufts University, observed, "The consequences would be enormous, with many problems emerging that we are currently unable to foresee. A problem we can predict, however, is major damage to our electorate, who will be increasingly distrustful of our major institutions (including media, scholars and government officials), and as a result less informed on the very issues that drive our democracy."

Kenneth Sherrill, professor emeritus of political science, Hunter College, City University of New York, said, "As people increasingly become unable to determine which information sources are trustworthy, they will decide that it is not worth their time and energy to do the work of figuring out what's true. Partisans will remain wedded to their trusted partisan sources. Others will drop out. Society will become more fragmented and civic engagement will decline."

Laurel Felt, lecturer at the University of Southern California, commented, "The consequences are dire because it disincentivizes following the news and/or acting on objectionable behaviors (e.g., miscarriages of justice, corruption, et cetera) because citizens may doubt that such flagrant offenses are being committed OR they may get the distorted sense that they happen all the time."

Peng Hwa Ang, an academic researching this topic at Nanyang Technological University, observed, "Interestingly, some research done suggests that it is not the burst of fake news (also known as public information by bad actors) that is the problem. It is the corrosive drip of such news that erodes confidence in democracy. The very bad outcome is the distrust in the democratic process. If we look at the U.S. and UK, the winner of both elections are those who want to erode such confidence."

Many said that when the public loses trust or when they are overwhelmed by too much contradictory input they will lose faith in the process and 'opt out' of participation.

C.W. Anderson, professor at the University of Leeds, wrote, "More and more people will opt out of civic engagement, and civic life, generally, as they become overwhelmed with separating signal from noise. It will simply become too much work. Which will leave people in charge who do not have the best interests of the general population at heart. Most likely, the polarization of American society will only spread further."

Justin Reich, assistant professor of comparative media studies, MIT, noted, "Autocratic societies have recognized that the most effective way to manage societal information is less about countering particular perspectives and more about flooding people's information channels with distraction, misdirection and falsehoods. In the absence of reliable arbiters of truth and falsehood, people are more likely to defer to tribal and ideological loyalties. Gary King has excellent research on state-sponsored social media propagation in China, showing that one of the central aims is flooding social media with noise and distraction."

A **professor and researcher of American public affairs at a major university** replied, "Perhaps the most troubling consequences are a general lowering of trust in institutions and withdrawal from public life. This creates a self-reinforcing spiral in which the least scrupulous people gain outsize influence on the political system."

A **professor of law based in North America** replied, "Many people will not trust the information, which makes it possible for rumor and innuendo to play an even bigger role than today. Policy making, already difficult, will become even harder. People will not trust."

David Brake, a researcher and journalist, replied, "Political debate will become increasingly difficult if both sides of the debate proceed from very different premises about the state of the world."

William Anderson, adjunct professor, School of Information, University of Texas-Austin, replied, "The primary consequence is that there will not be any large-scale society that shares common goods and common goals."

A **professor of information science at a large U.S. state university** wrote, "Consequences include a loss of trust in other people, in political powers and in countries."

An **author/editor/journalist** wrote, "There are forces both in the political spheres of the world and the natural spheres that are ongoing and untreatable without the collective strong-minded action of people. They require a determined and relentless response from humans to be overcome, and when humans are too busy fighting each other, there is scant energy left."

Social, economic and political inequities seen by some as a root cause

Societal inequities are seen by a share of the respondents as an underlying cause of much of the misinformation, the disagreements, the shrinkage of what might have been considered "common knowledge."

A **professor at MIT** commented, "We can look forward to intensified tribalism and a breakdown of a commonly held social norms… Some people may be dupes, but most are simply navigating the world in ways that they think make sense. Media don't 'do' things – people do. So let's push for economic and social equity, for inclusion, for critical thinking and solve the problem that way. Once we have systems that vet 'the truth,' you can be sure that power will find a way to use it to its own advantage. My 'truth' is invariably another man's

'lie,' so while we can and should have a pitched debate over truth claims, nothing beats an empowered, thoughtful and critical populace."

Jon Lebkowsky, web consultant/developer, author and activist, commented, "We're already seeing the consequences: deep polarization, suspicion, manipulation of public sentiment, erosion of rational civil discourse, widespread confusion and increasingly chaotic public/politcal spheres."

A **research scientist who works at Google**, said, "The consequence could be a two-class society where the competent minority is ruled by an ignorant majority."

A **partner in a services and development company based in Switzerland** predicted that using censorship as a tool will make things worse, writing, "Ultimately [the result of the expansion of misinformation will be] bellum omnium contra omnes – the war of all against all – as described by Hobbes. Of course society automatically creates new centers of power, making do with disparate inadequate tools if no orderly adequate ones are available. One such inadequate tool is censorship; it is likely to spread and further compound the problem of trust."

Sahana Udupa, professor of media anthropology at Ludwig Maximilian University of Munich, explained how the popularly used term "bad actors" would be better stated as "extreme speech" and then noted how inequities have eliminated some people. She wrote, "'Bad actors' is a highly political term and one cannot have a blanket approach to digital information based on a strict binary of bad and good. We have developed the concept of 'extreme speech' to understand how digital speech as a situated practice pushes the boundaries of legitimate speech along the twin axes of truth-falsity and civility-incivility. This means we remain aware of how 'bad actors' and 'hate speech' are framed in the first place. With such a situated understanding, digital speech practices should be mapped, and if found harmful for contextually rooted, historically sensitive reasons, one must raise strong barriers. The reason is such harmful content can render it so vulnerable groups and individuals (along the axes of caste, gender, religion, ethnicity, numerical majority/minority etc., and their intersections) are not prevented from participating in the public debate. The rise of right-wing populism and demonic majoritarianism have a lot to do with negative forms of extreme speech forced into the channels of digital media. Digital media consumers are not gullible. But trust networks are radically reconfigured in the digital age. What comes on Whatsapp is rarely disputed because messages are individualized and laced with multimedia enhancements which make it difficult to recognize and bust false and hateful narratives."

A lack of 'common knowledge' hinders finding common ground and common solutions

Larry Diamond, senior fellow at the Hoover Institution and FSI, Stanford University, observed, "If we fail in this task, social and political polarization will deepen because there will be no basis for common knowledge and understanding about any issue. Every political orientation will be living in its own information bubble, even more so than today. Distrust in institutions of all kinds will proliferate, and the ability of authoritarian regimes to subvert democratic practices, as Russia did with the 2016 elections in the U.S., will surge."

Maja Vujovic, senior copywriter for the Comtrade Group, noted, "The very fabric of society would unravel if the public could never trust public information. Worse yet, spurious agents could control large groups by serving them simplified or distorted information. People have proven severely susceptible to propaganda, over and over. Democracy gets deformed without independent information to guard it."

Steve McDowell, professor of communication and information at Florida State University, replied, "Without a common set of verifiable facts it is hard to have an informed public debate on problems and challenges confronting society, and to move from there to identifying priorities and crafting social or policy responses."

Alan D. Mutter, media consultant and faculty at graduate school of journalism, University of California-Berkeley, replied, "Loss of trust starts with diminished confidence in the truth of empirically indisputable facts like climate change or the brutal consequences of underfunding Medicaid. If we cannot agree on the facts, then we cannot have the sort of dialogue that produces good public policy and a healthy society. When truth is denied and trust is devalued, our democracy is at peril."

A **political science and policy scholar and professor** said, "The result could be the end of a shared reality, which makes it much harder to work together as a society."

Jeff Jarvis, professor at the City University of New York Graduate School of Journalism, commented, "The consequences are dire indeed: a failure of the public conversation and deliberation that is the engine of democracy. But beware the temptation to cry as journalists do, 'You'll miss us when we're gone.' Many would not. We must reinvent journalism for this new reality to truly serve diverse communities in society and to convene them into informed and civil conversation, not just to produce a product we call news that we insist the public must trust, or else!"

Geoff Scott, CEO of Hackerati, commented, "That depends on whether people choose to think critically and independently, pursue information from outside of their information bubble, and are open to having their minds changed. This is primarily and education and social challenge. If we can't address it at this level, bad actors will simply need to assert a narrative that serves their purpose and people will believe it."

Glenn Edens, CTO for Technology Reserve at Xeroz/PARC, "The continued fragmentation of information consumers is a serious issue. Society, of course, works best when there are a set of shared values, transparency and verifiable sources – we will have to adapt to this new world and the means are not clear yet."

Veronika Valdova, managing partner at Arete-Zoe, noted, "Disintegration of information environment to the point that there is no universally accepted picture of reality would have profound consequences on the functioning of the entire society. People act on information they have, they buy property, pursue careers, move around the country and the world, conduct business, undergo treatments, dedicate their time and resources to college degrees based on expectations and picture of the world they have. If there is no consensus on the basic understanding of reality, people cannot make rational informed choices relevant to their everyday life. At individual level, a prolific disinformation results in shattered reputation and loss of status, money, opportunity and life. Alternative information pipelines that develop in response to overwhelming amounts of falsehood in major media may be equally damaging."

Mark Glaser, publisher and founder, MediaShift.org, observed, "The consequences are terrible. Without having trusted information, it's difficult for many organizations to function properly including governments. We rely on factual information as a cornerstone of a functioning democracy."

Scott Spangler, principal data scientist, IBM Watson Health, wrote, "The loss of a common basis for fact and perceived reality will lead to greater and greater societal fragmentation and conflict."

Henning Schulzrinne, professor and chief technology officer for Columbia University, said, "It further degrades the notion of a common basis of fact for discussions of public policy and governance, as all information will be seen as equally suspect and untrustworthy, or as just an opinion, a matter of taste."

Paul Hyland, principal consultant for product management and user experience at Higher Digital, observed, "Civil discourse and political debate will be increasingly difficult or impossible."

Laurie Rice, associate professor at Southern Illinois University-Edwardsville, said, "When misinformation is common and widespread, trust in all sorts of sources of information – both good and bad – weakens. In addition, those lacking the tools, time, or skill to weigh and assess information from various sources can become more easily manipulated by bad actors."

An inability to trust is damaging to all human relationships and systems

Many respondents were most concerned with the loss of trust – not only in information but in other humans and in human systems.

Alejandro Pisanty, a professor at UNAM, the National University of Mexico, and longtime internet policy leader, observed, "The consequences of public information being coopted by bad actors are dire; a downward spiral of reinforced ignorance-bad judgment-generalized disbelief preys on the prejudices, bias and sheer lack of knowledge of large sectors and allows bad actors either to coopt them, or to be allowed free rein to govern and prey."

David Conrad, a chief technology officer, replied, "Trust in systems, processes, and institutions will continue to degrade, potentially leading to increases in demagoguery, extremism and civil strife."

Richard D. Titus, CEO for Andronik and advisor to many technology projects, wrote, "All societies are built upon trust. The Magna Carta, the Declaration of Independence – trust is critical to civil society. One need only look where the deterioration of trust occurs, Somalia, Syria, Venezuela and now ever the U.S. to see rising militancy, civil unready as the direct descendants of a loss of trust."

Erhardt Graeff, a sociologist doing research on technology and civic engagement at the MIT Media Lab, said, "Although mistrust can be used constructively to buttress democracy, when it is allowed to fester into chaos it poses an existential threat to the institution. The creation of chaos by seeding doubt and conspiracy theories – a highly refined strategy in Russian propaganda – allows authoritarianism to rise. When all facts are dubious and you cannot trust anyone, a broad power vacuum can emerge which entrenched powers and

charismatic leaders are poised to fill by promising nostalgic visions of strong-armed stability."

Sharon Haleva-Amir, lecturer in the School of Communication, Bar Ilan University, Israel, said, "The consequences depict a rather dark future of a more-polarized world; a world in which words, facts or truth have no meaning where people will not be able to cooperate for worthy causes as they will not trust one another and in which governments control citizens by spreading whatever news they want to. With no trustworthy media to count on, no democratic society could live on and prosper."

Sonia Livingstone, professor of social psychology, London School of Economics and Political Science, replied, "I have two kinds of anxieties: **1)** Bad actors in the sense of hackers, purveyors of misinformation, criminals will get dealt with by state-led systems of criminal justice and law enforcement; I'm more worried about. **2)** The commercial reshaping of 'information' in the interests of powerful private sector actors with a lot of lawyers and lobbyists. People already can't tell what's trustworthy or true, so probably those with knowledge will withdraw and find a niche alternative, while those without knowledge will withdraw and just become yet more disaffected; which will exacerbate inequality and disruption."

Hazel Henderson, futurist and CEO of Ethical Markets Media Certified B. Corporation, said, "As we have seen, whole societies can be disrupted, citizens mistrusting and informing on each other, these are the classic tools of takeovers by totalitarian leaders and authoritarian governments. George Orwell was right!"

Brooke Binkowski, managing editor of online fact-checking site Snopes.com replied, "Destabilization; chaos; bad faith; lack of national unity, which in turn further weakens the state; lack of trust in institutions within and without the United States; violence toward the most vulnerable (i.e., migrants and impoverished citizens)."

Larry Keeley, founder of innovation consultancy Doblin, observed, "In a word: Devastating. It will erode the basic check on power (governmental, corporate, institutional) that depends on trusted information systems. George Orwell's dystopian world becomes a reality – but far worse, since there will be many more ways for anyone with an agenda to find fanatical adherents. After a while, citizens, like in Russia or North Korea will trust no one."

George Siemens, professor at LINK Research Lab at the University of Texas-Arlington, commented, "Effective discourse across political party and other belief systems are at risk if

we are not able to create a trusted digital information ecosystem. The consequences of society will be a loss of many of the social and connected aspects of the internet as confidence will be stripped from these spaces. Dialogue will return to closed, trusted spaces with intermediaries (like with traditional media).”

Kenneth R. Fleischmann, associate professor at the University of Texas- Austin School of Information, wrote, “Certainly, there are egregious cases of introducing fake news to attempt to change the outcome of, for example, the 2016 election, particularly when it is apparent that much of this was done by or with the assistance of Russian hackers. However, any efforts to clamp down on such fake news might constitute a form of censorship that might undermine trust – there is a fine line between ensuring trustworthiness of public information and leading to a centralized government information system where there is only one trusted set of information (which is not necessarily trusted, on a deep level, by a large chunk of the population).”

Paul Saffo, longtime Silicon Valley-based technology forecaster, commented, “People focus on dramatic, extreme outcomes, but the greater danger comes from the insidious effects of cynicism and distrust engendered by an unreliable medium. The consequence will be increasing friction in social systems that in turn will retard the effective functioning of global civil society in the face of ever-growing complexity.”

Societies must support and turn to credentialed sources in the future – to 'trusted actors'

Many respondents pointed out that the overwhelming amount of information – “mis” and otherwise – about any topic today is part of the problem. They note that when people feel overwhelmed by information they often turn to social media echo chambers or other spaces where they can find familiar information with which they agree. They may often be misinformed or manipulated or just not get the chance to see other viewpoints fairly shared.

Irene Wu, adjunct professor of communications, culture and technology, Georgetown University, said, “Information and communication are the weft and weave of the social fabric. If they are unreliable, society cannot hold together. However, decentralization of power over information while allowing trusted institutions to emerge is a better path forward than centralizing the responsibility for good information with security services or with the government.”

An **anonymous respondent from the Berkman Klein Center at Harvard University** noted, "There have always been and will always be bad actors. The danger is in the unwillingness of the general population to accept responsibility for assessing the intentions, actions and information of those people around them. When the people won't accept that responsibility, a society can slip easily into group thinking or absolute rule by the minority who control the channels of information."

Alan Inouye, director of public policy for the American Library Association, commented, "One implication is that the general public will need to be increasingly more sophisticated about information and communication – being able to critically examine not only the content of messages but also the context in which they are communicated."

Sam Punnett, research officer, TableRock Media, replied, "The consequences are dire, leading to an erosion of social institutions. The outcome is a choice of choosing to be educated or choosing to be manipulated. Media/information literacy is essential in a society that generates so much of it. Put glibly, you are what you view. Information flow to the individual will only get increasingly customizable in the future. If one lacks the awareness of one's media diet then one gives little thought to the potential hazards of a 'junk' diet that feeds exclusively entertainment over that which feeds an informed citizen."

A number of respondents expect the reaction by some people to the recognition that there is a lot of misinformation out there will be a return to neutral information sources.

A **researcher at Karlsruhe Institute of Technology** replied, "Societies need to develop strategies – and can – to identify and tackle unwanted actions. One effect might be, that trust in established authorities will increase because they will be regarded as the only 'safe zones' in the otherwise wild information scape. This obviously requires that such authorities meet the expectations, otherwise alternative ('bad') actors might prevail."

An **associate professor at a major Canadian university** wrote, "We may see a shift back to notions of authority that drove pre-internet print publishing and journalism."

Leah Lievrouw, professor in the department of information studies at the University of California-Los Angeles, observed, "Bad actors have always attempted to capture and shape knowledge for their own purposes and gain, whether we call it revisionism, propaganda, spin, public relations, 'curation,' what have you. The question is whether, and which, information sources can be perceived as impartial, thorough, dispassionate, and fair. That's a cultural question: do we even want fair, impartial – modern – information sources? If so, we'll find or

create them. If not, no amount of technological intervention will magically ensure information quality."

Andrew Odlyzko, professor of math and former head of the University of Minnesota's Supercomputing Institute, said, "We in an environment of information and misinformation. We will simply have to learn how to choose the webs of trust we rely on."

Geoff Scott, CEO of Hackerati, commented, "That depends on whether people choose to think critically and independently, pursue information from outside of their information bubble, and are open to having their minds changed. This is primarily and education and social challenge. If we can't address it at this level, bad actors will simply need to assert a narrative that serves their purpose and people will believe it."

Jim Hendler, professor of computing sciences at Rensselaer Polytechnic Institute, commented, "We will need to develop social and community mechanisms to try to deal with this – the problem is not new to digital media, propaganda, for example, has been around a long time – the bigger issue is whether newer and faster ways of distorting information can be countered by newer and faster ways of providing balance."

Liam Quin, an information speciliast with the World Wide Web Consortium, noted, "What we need is not to prevent lies, but to make it easier to find out whether something is true."

The **assistant director of a digital media and learning group** at a major U.S. university, said, "It's critical to have journalism organizations such as the Washington Post continue to fight to provide deep and critical political coverage. The consequences of not supporting an independent press are a lack of a public record, the inability to provide a coherent approach and narrative to a variety of issues, as well as the broader enterprise to keep in check immoral and incompetent government entities, corporations and bad actors."

Jeff Jarvis, professor at the City University of New York Graduate School of Journalism, commented, "The consequences are dire indeed: a failure of the public conversation and deliberation that is the engine of democracy. But beware the temptation to cry as journalists do, 'You'll miss us when we're gone.' Many would not. We must reinvent journalism for this new reality to truly serve diverse communities in society and to convene them into informed and civil conversation, not just to produce a product we call news that we insist the public must trust, or else!"

This is the human condition – misinformation lives. Some choose to expect or at least remain optimistic that 'truth wins out'

A share of respondents said while the information environment today is distressing it exhibits typical behavior that has been made more visible due to technological change.

Stephen Downes, researcher with the National Research Council of Canada, commented, "The co-opting of public information by bad actors has already taken place, and has been the case for a long time. The internet did not create this phenomenon. We know what happens – wars are started based on fake stories, mass persecution of races, religious or political groups takes place, the environmental and health impacts of dangerous chemicals and processes are ignore – etc. The history of information before the internet is full of such cases. What is new is **1)** the means to create disinformation have become democratized, but **2)** so have the means to detect it."

Matt Armstrong, an independent research fellow working with King's College, formerly executive director of the U.S. Advisory Commission on Public Diplomacy, replied, "The society will be co-opted. The naive, the angry and the shortsighted will be enlisted in support of bad actors, and any wake-up or regret will come too late. This is not new, despite our attempts to frame this issue as unusual and unique to our age."

Francois Nel, director of the Journalism Leaders Programme, University of Central Lancashire, noted, "(With apologies to the Bible) like the poor, bad actors and taxes will always be with us. And we have, and will, continue to cope."

David C. Lawrence, a software architect for a major content delivery and cloud services provider whose work is focused on standards development, said, "It maintains the status quo of human social life throughout our entire existence as a species, and that's probably for the better. Knowing that you have to be prepared for the possibility that someone is misleading you is better than trusting everything and then ultimately being taken advantage of when the bad actors find a way to get their message out."

John Lazzaro, a retired electrical engineering and computing sciences professor from the University of California-Berkeley, wrote, "Society will develop antibodies: skepticism, common sense, 'extraordinary claims require extraordinary proof.' For a real-world analogy, the rise of the three-card Monte con in the New York subway in the 1970s did not lead to an economic catastrophe."

Scott Fahlman, professor emeritus of AI and language technologies, Carnegie Mellon University, pointed out that media-based information always been manipulable but the explosion of information has complicated things, writing, "We have moved from a world with just a few news outlets, trusted by some and able to manipulate public opinion to a more diverse and democratic system in which everyone can spread their opinions (and deliberate lies if they choose to). We have seen that it is now much harder for people to decide what to believe, and many people no longer make the effort, just living in their own echo chambers."

Brian Harvey, teaching professor emeritus at the University of California - Berkeley, said, "There's nothing new about 'coopting of public information' except, maybe, that the internet lets non-rich people play. The best vaccination I know of against fake news is to study Marx and understand the class structure of society, but this is pretty much a non-starter in the U.S."

Tom Rosenstiel, author, director of the American Press Institute, senior non-resident fellow at the Brookings Institution, commented, "Over the stretch of history, I think the signals are fairly clear. It requires political leadership, and cooperation by political leaders, to blunt the effect of misinformation. It is not going to be something that technology can solve, though it is something technology can make worse. Will the political parties and political leaders exploit the innate potential of citizens to believe false rumors, or will they try to rise above it."

A selection of additional remarks on historical context:

- An **anonymous professor of media and communications** commented, "It will continue as it always has. Truth is not a necessary condition for social function."
- The **dean of one of the top 10 journalism and communications schools in the U.S.** replied, "Thinking that today's 'fake news' is different from other major points in history is silly. We've always had enormous sources of fake news passed along one-to-one, by bad sources, through misleading PR efforts, by phone, by fax, by penny press, by party press, by McCarthyism and similar efforts, even in religious venues. We always believed that 'truth and falsehood grapple,' only that we are optimistic that truth eventually wins out."
- And an **anonymous CEO and consultant** based in North America said, "This has been a problem since Man started communicating in a physical medium. We have yet to figure out how to deal with bad actors."
- An **independent journalist** and longtime Washington correspondent for leading news outlets said, "The consequence? It's called life."

The jury's out on whether any actions taken could have net-positive results

Whether they predicted that it won't improve or it will improve in the next decade, the vast majority of respondents wish for a better information environment in the future but are unsure if it can be achieved.

Sandro Hawke, a member of the technical staff for the World Wide Web Consortium, shared a common point of view in writing, "If we let bots, people with psychosis and enemy agents (whoever that might be in the given context) speak with the same voice as members of our communities, the damage will be incalculable. Literally, the end of civilization, I expect. We have to maintain strong attribution and reputation elements in public discourse. We have to be clear who is saying what, and how it fits in with how they've behaved in the past."

The majority of respondents indicated they would like to see more people actively thinking through the possible ways to enhance the information environment, but some expressed doubts that much can be done without causing other negative effects, and some said human nature is such and the advances in the weaponization of technology are such that the current information atmosphere may not be something that can be improved upon.

For instance, in their answers to this and all questions in this canvassing many expressed doubts in the public's willingness to pursue and consume a more fact-based information diet, no matter how much information literacy is emphasized in society.

Fred Davis, a futurist based in North America, predicted that if the current information environment is extended, "Mass media becomes even more propaganda-oriented. Social media creates the potential for 'society hacking.' One of the big problems of fake news is that it also casts doubt on real news."

Giacomo Mazzone, head of institutional relations for the World Broadcasting Union, was pessimistic about people pursuing the most-reliable facts, writing, "The problem is that today's society is hungry for fake news. It's not looking to stop it."

Some expressed concerns that regulatory fixes, legal changes, filtering, flagging and other suggested remedies will have their own drawbacks while possibly not having enough impact on extreme actors' manipulation of the information environment.

Isto Huvila, professor of information studies, Uppsala University, replied, "The consequences [of misinformation in the next decade] will be disruptive but at the same time, authoritarian measures to prevent them can be equally bad."

Micah Altman, director of research for the Program on Information Science at MIT, commented, "Judge Brandeis said, 'If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence.' The results of either dominance of false information or silencing of 'bad' speech would be to severely impair liberal democracy."

So, once again, the question is: What are the consequences for society if misinformation continues to expand?

Paul N. Edwards, Perry Fellow in International Security, Stanford University, commented, "Political divisions will be exacerbated and splintered into many factions, each with its own preferred sources of information, verified or not. As at present, wealthy and powerful actors will learn to shape public opinion through disinformation in order to promote their views and values."

Susan Etlinger, industry analyst, Altimeter Research, said, "To be blunt, I think we're living it right now in many places in the world. And we've seen this before: erosion of human rights, weakening of the rule of law, suppression of free speech; all of these are symptoms of weakened public institutions and values."

Andrew Nachison, author, futurist and founder of WeMedia, noted, "The result can be civic collapse, dark ages, widespread distrust of the other."

Mohamed Elbashir, senior manager for internet regulatory policy, Packet Clearing House, noted, "Fake news/information could lead to catastrophic outcomes, spread hate speech, incite violence and undermine the core values of the peaceful exchange of conflicting ideas and opinions."

Robert W. Glover, assistant professor of political science, University of Maine, wrote, "The complete breakdown of our political system, not to mention vulnerability in our basic social structures and economic system."

Tony Smith, boundary crosser for Meme Media, commented, "Accelerating backslide towards authoritarians by noisy idealists of all flavours."

Tim Bray, senior principal technologist for Amazon.com, wrote, "Damaging political ideas having influence over enacted policies."

Joseph Turow, professor of communication, University of Pennsylvania, commented, "The escalated distribution of concocted facts casting opponents in a negative light will often mean that various actors will be able to use social media, off-the-beaten-track sites and apps, and email to reinforce silos of opinions regarding issues of concern to them. They will also at times be able to short-circuit political compromises across sectors of a society by planting widespread, reasonably plausible stories that sow distrust."

Wendell Wallach, a transdisciplinary scholar focused on the ethics and governance of emerging technologies, The Hastings Center, wrote, "Power will remain in the hands of the powerful, or those best able to exploit the technology in pursuit of their own goals and ideology."

Amy Webb, author and founder of the Future Today Institute, wrote, "AI agents will help to create stories, distribute content and eventually personalize it for each individual news consumer. Without action today, in the future more our own opinions will be reflected right back at us, making it ever more difficult to confront contrary beliefs and ideologies. Extreme viewpoints will feel like the norm, not the outliers they actually are. Leaders – and everyday people – should base their decisions in fact, but we're still human. Emotion gets in the way. I foresee extreme viewpoints and personal duress shaping our future world, and that should be a grave concern to us all."

Jim Warren, an internet pioneer and open-government/open-records/open-meetings advocate, said, "IF so, the results have been, are, and will be Orwellian until citizens overthrow the perpetrator(s) – which can take generations. The consequences of citizens – individually and collectively – being unable to prevent co-opting of information by bad actors would (or will?) be what it has always been: tyranny and citizen 'helplessness' until they (we!) revolt and redress the abuses."

A **global telecommunications leader based in Central America**, commented, "Societies need to put in practice ways and means mainly through education, formation and training to lessen the impact of bad consequences. Societies need to find appropriate incentives. Defense and attack will gain in sophistication over time."

Susan Price, lead experience strategist at Firecat Studio, noted, "Anything created by humans can be hacked; protection must be based on the cooperation of motivated humans."

Johanna Drucker, professor of information studies, University of California-Los Angeles, commented, "We are already seeing those consequences – a form of affective fascism that works through a phantasmatic force. How to counteract this? We can only hope that some recognition that human survival depends on responsible cooperation – among humans, but also between humanity and the ecology on which it depends – will have sufficient persuasive force to prevail."

A selection of additional comments by anonymous respondents:
- "Economic terrorism generally leads to dictatorship."
- "The dream for the internet was that it would give a wider range of viewpoints but instead it has created an echo chamber for false stories."
- "Making decisions based on bad information is bad for everyone. The consequences are incalculable."
- "As long as information systems are hiding their selection and computing mechanisms, it will be impossible to prevent the coopting of public information by bad actors."
- "It's the rise of 'personal truth' over verifiable truth."
- "Parts of the e-economy may slow or regress."
- "Disinformation fatigue may lead to new forms of post-information politics."
- "[There will be] more opportunities for demagogues and corruption in general."
- "The result is a society that is based on fear, rather than trust. Where no accurate measure of public opinion is possible because of propaganda, echo chamber and spiral of silence effects."
- "Powerful people with strong financial interests will control our democracy even more and hate groups will take advantage more to increase polarization."
- "Chaos." (this was the response of several respondents)
- "A race to the bottom in government and big industry, where anything goes."
- "Low-information voters will continue to vote for liars. Society will suffer. There will be more division between information-have and information-want-nots."
- "Manipulations will be more sophisticated than most of us can imagine, or detect."
- "Cheap, intolerable interference by foreign governments."
- "Echo chambers, fear mongering, prejudices, racism, social disintegration, mistrust in fellow citizens and political institutions."
- "Election of demagogues. Isolationism and conflict. Decline of science."
- "A breakdown of democratic norms and values, and increased power for those who don't care what 'truth' is."
- "The danger is that this becomes a self-perpetuating cycle of ignorance."
- "It will take years for a social norm or technology to adjust to the current climate."

- "We live with it, just as we do with crime."
- "It's business as usual."
- "This is no worse than the impact of bad actors throughout history. In other words, sometimes terrible, but generally just a drag on the system."
- "The coopting of public information will be less effective over time. Shock value is not something that you retain over repeated abuses."
- "Were things ever so much better? Some features of the technology lead us to misjudge and exaggerate, change and overreact."
- "The cure is worse than the disease. Unless you want a 'Pravda' future, let democracy and freedom of speech work."
- "Society has to cultivate responsible and thoughtful people."
- "We are going to have to redefine how democracy can work."

<u>Follow-up #3:</u>
If changes can be made to reduce fake and misleading information, can this be done in a way that preserves civil liberties? What rights might have to be curtailed?

While a number of participants in this canvassing say the protecction of civil liberties online is paramount, some said such sacrifices are necessary. Some experts warned that many of the proposed remedies to perceived problems in the information environment are likely to cut into free speech rights, broaden the already wide scope of online surveillance and greatly narrow the public's options for sharing opinions and information online anonymously. Anonymity has been most highly valued because it can protect whistleblowers, those subject to authoritarian rule and those subjected to discrimination. Some said that those who wish to spread misinformation will easily route around any changes and sacrifices of civil liberties will result in a net-negative impacts for society. The overarching trends in their answers are covered by these three quotes:

- A longtime **U.S. government researcher and administrator** in communications and technology sciences said, "Changes should *not* be made, because civil liberties would be curtailed."
- A **technology analyst** for one of the world's leading technology networking companies replied, "I don't know what changes would be effective."

- **Matt Mathis**, a research scientist who works at Google, said, "The right of free speech should not include global broadcasting of outright lies."

Leah Lievrouw, professor in the department of information studies at the University of California-Los Angeles, argued, "The authenticity, veracity, consistency, balance, fairness, et cetera, of information have, historically, been the responsibility of trusted institutions and actors (science, law, the academy, the press and publishers) who created systematic methods for making information as reliable as possible (though never perfectly so, which is more or less impossible). Peer review, editorial judgment, logical argument and debate have been our best tools – but all are now being undermined as 'elite' and thus illegitimate, in favor of emotion, personal-experience storytelling."

Marc Rotenberg, president, Electronic Privacy Information Center, wrote, "The meaningful solutions to fake news do not pose a risk to civil liberties; they pose a risk to corporate dominance of the internet."

Jim Hendler, professor of computing sciences at Rensselaer Polytechnic Institute, commented, "The only ways to fully curtail fake and misleading information (assuming such could even be rigorously defined) would be to rely heavily on rules and regulations that would be unacceptable civil liberties violations. What *can* be done is stronger policies that fight deliberate manipulation for profit or personal gain – many such laws already exist (libel and slander, SEC rules, et cetera) but the changing pace of technology means these rules need to be updated. Further, the mechanisms in the current legal system (for example, a libel case lasting years) cannot keep up with the pace of information – either much stronger penalties for convictions, new civic means of engagement, et cetera, would be needed."

Rajnesh Singh, Asia-Pacific director for an internet policy and standards organization, observed, "As the online population grows this will get more complicated."

Christian H. Huitema, past president of the Internet Architecture Board, commented, "I am very worried that in the name of 'banning fake information' we will get some kind of 'thought police.' Or maybe just speech codes."

Jamais Cascio, distinguished fellow at the Institute for the Future, wrote, "If the system changes to *prohibit* or otherwise *stop* the production and proliferation of misleading information, then this will undermine civil liberties, as the definition of 'misleading' will inevitably take on subjective qualities. If the response to misleading information is functionally-mandatory verification information, then this would arguably not violate civil

liberties. As long as the tools/methods used to reduce fake/misleading info do not *prevent* the discussion or creation of fake/misleading info, civil liberties will likely be fine. That is to say: a system that identifies false info without preventing the false info from being said would likely be civil liberties-friendly (or at worst, a frenemy). It's the prevention of communication that's the problem."

Amy Webb, author and founder of the Future Today Institute, wrote, "We humans have agency. We have a stake in what's coming next. The future is our shared responsibility in the present. We must engage in a difficult conversation about what constitutes 'speech' in the near-future AI age – and whether 'freedom' should be interpreted as broadly as it has in the past. Could the founders possibly have imagined a future of algorithmic subterfuge? And what happens when our AI agents start making unsupervised decisions? How do civil liberties apply then? The world is vastly complicated – too complicated for many of our current laws. While Congress may not enact a law abridging the freedom of speech, should there be a new terms of service – a new operating agreement – governing how information spreads for the 21st century? I think so."

John Anderson, director of Journalism and Media Studies at Brooklyn College, City University of New York, wrote, "The fact that we're raising the issue of curtailing civil liberties in order to better manage information flows suggests that this problem has already caused irreparable harm to norms of a functional democracy."

Andrew Nachison, author, futurist and founder of WeMedia, noted, "What are civil liberties in networks and communication systems controlled by private enterprises? We need a global doctrine for digital rights – and without that, civil liberties will be under constant threat from governments with authoritarian, anti-democratic instincts and policies."

John Markoff, retired journalist, formerly technology reporter for the New York Times, said, "This will be an enduring paradox. I believe we can have a more 'secure' computing universe, but only at the expense of traditional civil liberties."

David Weinberger, writer and senior researcher at Harvard's Berkman Klein Center for Internet & Society, noted, "We at least need to be asking about whether we can reduce the influence of false information while preserving robust, genuine disagreement."

There is likely to be a curtailment of the 'rights' of those who do harm to society

Some respondents said certain speech that is deemed to be a danger to society in some regard should possibly be limited.

Sonia Livingstone, professor of social psychology, London School of Economics and Political Science, replied, "Offline, no-one ever said they have the right to shout into the homes and private lives of everyone; the internet has amplified the ability of those with money to reach many ears, but I do not agree that's a speech right. So yes, 'speech rights' will have to be curtailed. But that will curtail the rights of the superrich, the malevolent and the private sector. Ordinary folk with something to say will still be able to speak, just not to reach absolutely everyone in an instant without any kind of filter for validity or relevance."

Joshua Hatch, president of the Online News Association, noted, "The 'actual malice' standard may need to be revisited. Even suggesting that makes me shudder, but I do think that ought to be considered."

Carol Chetkovich, professor emerita of public policy, Mills College, commented, "We need to have more public conversation about where we draw lines around 'free speech.' It's never been an absolute right, but we are facing particularly difficult challenges now in figuring out how to shape this right. Doing so will require dialogue. I suggest as a starting point thinking about Jurgen Habermas's 'ideal speech situation.'"

Mark Glaser, publisher and founder, MediaShift.org, observed, "You must preserve civil liberties at all costs no matter what you're trying to accomplish. However, there might be less 'free speech' for those who are using that as a shield to promote misinformation and fake news (along with hate speech)."

An **anonymous respondent** wrote, "It might cause a re-thinking of civil liberties; perhaps we need to know that an individual or a group, even among the young, have been responsible for creating false and misleading information."

Wendell Wallach, a transdisciplinary scholar focused on the ethics and governance of emerging technologies, The Hastings Center, wrote, "Freedom from repression can be maintained, but the freedom to pursue whatever one wants, even when this may harm others, would need to be curtailed. Those with the power to exploit the technology will resist such a curtailment."

Steven Miller, vice provost for research, Singapore Management University, wrote, "Maybe total unrestricted civil liberties are not the number-one priority. Maybe there are some reasonable trade-offs between absolute civil liberties (so-called freedom of speech and expression) with responsibilities for accuracy, verification, validation. In other words, in the U.S. now, there is 'freedom of speech,' but no requirement that people be responsible for what they say. This is an odd type of freedom, and does not necessarily serve the needs of the society as a whole. So there needs to be a stronger linkage between the freedom and the responsibility. I do not see this as a curtailment, but as an alignment that has been needed for a long time now."

Raymond Hogler, professor of management, Colorado State University, replied, "All increases in trust come at the cost of decreases in liberty."

Sam Punnett, research officer, TableRock Media, replied, "Unfortunately the only way to reduce misleading information is for there to be consequences for its knowing creation. It is difficult to foresee how the future of the news media will evolve (particularly in the United States) given the continuous stream of contradictory statements and lies issuing from formerly reliable institutions such as the U.S. presidency. There will likely be eventual consequences, but the fourth estate and government institutions in the U.S. are struggling to adapt. Freedom of the press and free speech in a democracy are sacrosanct. Speech is not something you can easily legislate – neither is media consumption. In a democracy you have the freedom to be uninformed and the freedom to only consume what feeds your existing biases. The consequences may well be to lose your democracy, herein lies the paradox."

Bart Knijnenburg, researcher on decision-making and recommender systems and assistant professor of computer science at Clemson University, said, "There are too many people nowadays who don't understand that freedom of speech is not the same as having a right to claim a platform. If your speech is asinine, hateful or plain wrong, you cannot be angry at others for denying your voice to be heard."

Mike Roberts, pioneer leader of ICANN and Internet Hall of Fame member, replied, "The First Amendment provides a lot of space for argument over its rights and obligations. Other countries have stronger defamation and libel laws, and moving ours in that direction should be considered."

Mercy Mutemi, legislative advisor for the Kenya Private Sector Alliance, observed, "Controlling fake news whilst preserving civil liberties is a balancing act. This would mean

deliberately denying some posters the right to post information online. It would definitely mean compromising the freedom of expression and in a way the right to access information."

Jan Schaffer, executive director of J-Lab, said, "The right to lie and the right to misstate information might need to be curtailed, with fines or loss of access to public airwaves and/or cable, internet. I don't think the use of public airwaves (broadcast television/radio/Sinclair-type ownership) should be granted to those shown to have used them to disseminate false information."

Erhardt Graeff, a sociologist doing research on technology and civic engagement at the MIT Media Lab, said, "Avoiding trampling on civil rights, particularly the strong definition of freedom of speech in America, will be extremely tricky. Following President Trump's repeated accusations of fake news from American journalists, leaders less unencumbered by strong civil rights statutes in their own countries quickly adopted the 'fake news' frame to go after inconvenient journalists by creating new regulations such as whitelists for approved news organizations. Any attempt to regulate misinformation that appeals to the 'common or public good' or classifies comments as reckless or negligent can and will be manipulated by policymakers to police dissent. Privacy protection is another obvious target that could erode in the name of fighting misinformation. Journalists' shield laws have started taking a beating, but we should expect that attempts to root out anonymous and pseudonymous sources of misinformation online could undermine the privacy of all users and creating chilling effects on free speech. As the issue of online harassment has shown, there is a need to revisit how we conceive of civil liberties in these contexts, but we must proceed with extreme caution."

Joel Reidenberg, chair and professor of law, Fordham University, wrote, "Freedom of expression and censoring fake and misleading information are mutually exclusive."

Systems should generally be optimized in a way that protects civil liberties

Micah Altman, director of research for the Program on Information Science at MIT, commented, "Supporting an independent media and robust information systems that are open, transparent, and traceable to evidence is compatible with civil liberties. Silencing bad speech is not – and doesn't work."

Nick Ashton-Hart, a public policy professional based in Europe, commented, "The idea of balance between other priorities and civil liberties is a false one. Rights are not something we

use as currency; they are integral. We need to approach rights and other public policy goals from a win-win perspective, where solutions to problems reinforce rights, not reduce them."

Brian Cute, longtime internet executive and ICANN participant, said, "I don't support curtailing civil liberties as a solution to societal challenges."

Larry Diamond, senior fellow at the Hoover Institution and FSI, Stanford University, commented, "Yes, I strongly believe that freedom of expression can and must be protected. But this does not mean that any terrorist or propagandist has the right to say literally anything, no matter how violence-inducing or patently false it may be, AND have it be given the same level of search priority and accessibility. I believe we can find a reasonable balance here, and again, that civil society and the internet companies must be in the lead, with government as a consulting but not dictating partner."

An **anonymous respondent affiliated with the Berkman Klein Center at Harvard University** said, "We can institute penalties for people who knowingly spread false information to gain power, influence or wealth. But we also run the risk of quelling a free and fair exchange of ideas and information. The dangers to a population's civil rights are too great to balance the potential gains of those laws."

Alan D. Mutter, media consultant and faculty at graduate school of journalism, University of California-Berkeley, replied, "Curtailing free expression would be more dangerous than anything."

Jane Elizabeth, senior manager American Press Institute, said, "This can be done in the same way we manage the conflicts inherent in free speech. Yes, it can be messy and difficult, but the First Amendment has been in place since 1791 and, all in all, it's served us pretty well."

Nate Cardozo, senior staff attorney, Electronic Frontier Foundation, observed, "The inevitable outcome of any system that aims to reduce the reach of fake news will be the reduction of expression of all kinds. It's simply incompatible with free speech."

Diana Ascher, information scholar at the University of California-Los Angeles, observed, "Until systemic discrimination is addressed, even new means of documentation that provide 'incontrovertible' evidence will be of little value in holding authorities accountable for violations of civil rights. For example, video footage of police brutality in the deaths of people of color has done little to dismantle structural racism, despite widespread news coverage. In

2016, there were 1,092 police killings of African Americans in the United States. Thus far, not one officer has been convicted. The Federalist direction in which the Trump administration has moved only exacerbates this through the creation of systems to identify and track populations of color."

David A. Bernstein, a marketing research professional, said, "I believe it is possible by assigning some sort of a truth or consistency score to statements similar to what we saw by FactCheck during the past political debates. Why can't we create a system that would be the Consumer Reports of fact-checking? I do not see any civil rights or freedom of speech problems. You can still say what you please, but then you have to live with the scoring by an independent scoring agency."

Patrick Lambe, principal consultant, Straits Knowledge, noted, "Machine intelligence and knowledge-organisation techniques, together with human supervision are now smart enough to identify characteristics of false messaging based on the message and its manner of diffusion alone, without attending to privacy of originators or diffusers. Without diffusion, the incentive to create false messaging evaporates."

Daniel Kreiss, associate professor of communication, University of North Carolina-Chapel Hill, commented, "I do not think the issues are legal, so I do not think civil liberties or rights are really at issue. The news media can, and should, change its patterns of coverage to: 1) Represent a broader range of intra-party and intra-social group debate and diversity of thought, especially when factual issues are at stake. 2) Highlight intra-party critiques of elites, especially when the veracity of information is at stake. 3) Hire more journalists from the communities media outlets serve to deliver information and correctives in an identity-congruous way to audiences. And 4) make a solid distinction between freedom of speech and freedom of the press, with the latter being delimited to speech that the public needs to hear (which means not covering misinformation). Technology platforms should think about more transparency in terms of their policies around expression, make more data available around these issues, and think more creatively about how social identity shapes epistemology, not simply rely on professional journalism outlets."

David Manz, a cybersecurity scientist, replied, "Why do people assume security vs. freedom is a tradeoff? Privacy and security are on the same side. You cannot have privacy without security. INsecurity is opposed to privacy. This will not require any curtailment. Rather it will require a populous who wants to know where their information comes from. And a mechanism to share that information – something as simple as a Google search response of advertisements and legitimate results. Most savvy users can discern the difference easily.

Alternatively we can have complex roots of trust with certificates and authorities to validate from reporter to bureau, to editor, to consortium to outlet to reader."

More suggestions for potential solutions are included in another section, below.

It is not easy to define what is real, what is misleading. Who gets to decide?

Respondents pointed out that differences between the digital age and earlier times complicate already complicated issues tied to limitations to free speech: How do you determine who posted the information in question? How do you define "damaging" misinformation? Who gets to decide what should or shouldn't be classified – under any definition – as information that is false or damaging to society?

Stephen Downes, researcher with the National Research Council of Canada, commented, "The big difficulty in any campaign to reduce fake and misleading information will be to define what is real and not misleading. This isn't a free-speech question – we have plenty of safeguards against libel, slander, mischief, et cetera. What we don't have agreement on is on what counts as true – or, may be more accurately, how much fabrication is allowed. Should there be criminal prosecutions for denying human-caused climate change? Should people go to jail for advocating boycotts or divestment campaigns? Should religion be required to offer proof of its claims? Et cetera."

Jack Schofield, longtime technology editor at The Guardian, now a columnist for The Guardian and ZDNet, commented, "I can't see any way to stop the distribution of fake news for two reasons. First, everyone's a publisher, in the sense that they can post on social media. Second, some people don't think they are spreading false information: they genuinely believe crackpot conspiracy theories, and they refuse to accept provable facts. If you correct them, many just double down on their false beliefs. This is a problem that neither education nor honest media can solve."

Johanna Drucker, professor of information studies, University of California-Los Angeles, commented, "The dilemma is that all structural controls can be subverted, and that the more malicious and pernicious players are most likely to do so. The most effective method of guaranteeing the future of responsible journalism is through professional organizations and their certification/validation of sources/outlets. We have accreditation in other fields. We may need it in the domain of news and reporting. But what is to stop a bogus organization

from setting itself up as an accreditation agency? What political litmus test is applied? How to police partisanship when it aligns with the basic notion of what constitutes verity?"

A **distinguished professor of computer science and engineering at a major state university** noted, "Any authority that can prevent dissemination of fake or misleading information can also be used to prevent dissemination of legitimate information. Even public consensus technologies may simply be coopted by a wrong majority (remember, in the U.S. we had a majority belief for a period that blacks were subhuman)."

An **anonymous business leader** wrote, "The problem is who decides what is 'fake?'"

The **CEO of a major American internet media company** based in New York City replied, "The solution isn't censorship, it is about what gets magnified and promoted. People should be able to have wrong ideas, expound conspiracy theories, et cetera, but those views shouldn't be magnified by algorithms and media networks!"

Mark Lemley, professor of law, Stanford University, observed, "There is a great risk in having the government decide what news is real. Just look at who would be making that decision in 2017. When a government has an incentive to promote fake over real news, giving them the power to suppress or select news is a real danger. We are much better served by private, competitive rating systems."

Dave Burstein, editor of FastNet.news, said, "Any system will make it much harder to comment anonymously and free from government. Going beyond fraud to hateful or false claims inevitably will censor a great deal of legitimate commentary, I believe. The volume posted on the Net is so much [that] algorithms inevitably overreaching and inaccurate is the only practical technique."

Bernie Hogan, senior research fellow, University of Oxford, said, "Fake news is less an issue than the profiting off of misleading and sensational news that erodes trust in public institutions. This creates the seedbed in which absurdist conspiratorial positions are grown. The notion that we would curtail civil liberties assumes we need real names in order to discipline trolls. Really, we already know that those who are the most nefarious are doing so through legal means, shell companies, lobbyists and legislators. Through legal means they redistribute money and attention, manipulate citizens and callously look askance at unequal outcomes. The threat from Rupert Murdoch's demonstrably biased 'reporting' conglomerate is much greater than some online trolling by foreign actors. Curbing civil liberties is another

way of suggesting that the disempowered are the problem and it is their rude online comments that must be disspelled, when it is the powerful who are doing the exploiting."

Mark Bunting, a senior digital strategy and public policy advisor with 16 years' experience at the BBC, Ofcom and as a digital consultant, wrote, "The need to draw an appropriate balance between freedom and restraint is not new – it's been a feature of information environments as long as humans have had the means to communicate to co-opt support and coordinate against enemies. The crucial thing is to see this challenge as a matter of degree, not absolutes. The internet has enhanced opportunities for freedom and infringement of rights – we have to recalibrate our instruments for this new world, but we don't have to invent completely new science."

Alexios Mantzarlis, director of the International Fact-Checking Network based at Poynter Institute for Media Studies, commented, "Truly 'fake' information should be relatively easy to address without real consequences on civil liberties. Email largely defeated spam, for instance. But the misinformation space is a lot broader than totally fabricated stuff, as is made perhaps most clear by the taxonomy developed by Claire Wardle of First Draft. Truth comes in shades of gray and every item of information can be deemed at least somewhat misleading by someone. I am wary of any solutions that suggests basic legal rights need to be curtailed."

Eric Burger, research professor of computer science and director of the Georgetown Center for Secure Communications in Washington, DC, replied, "Who defines 'fake news'? Censorship that seems benign is the door to censorship that is malignant."

Barry Wellman, internet sociologist and virtual communities expert and co-director of the NetLab Network, said, "I don't trust self-serving governments deciding what's false and misleading information. I'd rather freedom of speech be preserved."

Glenn Edens, CTO for Technology Reserve at Xeroz/PARC, said, "Better internet protocols could help (CCNx for example where publishers can be verified), however this does address the issue of what sources individuals choose to trust. The solutions do appear to be as bad as the problem, especially related to free speech and civil liberties. Even a 'rating' system of trusted sources is questionable – rated by who?"

Michele Walfred, a communications specialist at a major U.S. university, said, "The concern in policing is having a police state and condemning free expression one that does not agree with as 'fake.' Opinion and satire needs to be labeled because although it should be

intuitive or obvious, it isn't. The identity of the publishers, their investors or backers should be fully disclosed. People are allowed to have left or right views. People are allowed to be vegan or not, et cetera. Skepticism of factual, peer-reviewed, researched articles is growing. Say what you want, but there should be a Better Business Bureau-type rating system – but who does that rating? It is a troublesome situation – when is an opinion a lie and an untruth? I don't know."

Helen Holder, distinguished technologist for HP, said, "Restrictions on the publication of patently false information probably cannot be done without infringing on civil liberties, except in cases of fraudulent advertising or incitement to violence. Despite the obviously negative impacts of trolls and other misinformation generators, it would be nearly impossible to curtail or censor them if no fraud or violence were involved because although there is a generalized damage to society from these practices, the direct, specific harm from each source is small and would be difficult to assess or prove."

Joseph Turow, professor of communication, University of Pennsylvania, commented, "Some social media firms are trying out algorithms aimed at identifying bad actors, not just content, by the size and formulation of their message traffic. But the statistical nature of this activity inevitably means good actors will be identified incorrectly. If governments get involved the cure might exacerbate the disease. Unscrupulous politicians in the U.S. and elsewhere would inevitably look for ways to tar opponents with the fake-news or (especially) weaponized fake information label and thereby pollute the media environment even more."

Greg Wood, director of communications planning and operations for the Internet Society, replied, "Centralized systems for authenticating or verifying information would seem to be unworkable and, as history has demonstrated time and again, incompatible with the individual civil liberties. A distributed approach to at least authenticating the sources of information might be possible."

Brad Templeton, chair emeritus of the Electronic Frontier Foundation, said, "In the U.S. and many places, freedom of the press must be maintained. That means systems that tag misleading information will not be legally required, but this does not mean they can't be commonly used. However, there will be those who correctly and incorrectly criticise the flags of such systems as politicized, which will drive some away from them."

Michael Rogers, principal at the Practical Futurist, wrote, "This is a bigger problem than even the technology, especially for democracies. There would need to be complete transparency around reasons for information rejection, as well as a public appeal process.

There are precedents within democracies for fake information control, such as Holocaust denial. Achieving a system that respects civil liberties would require a very careful coordination of technologists and elected officials."

The recalibration will have to include new approaches to machine-generated speech. A leading **researcher studying the spread of misinformation** observed, "This will be a difficult challenge, and possibly one of the defining regulatory and policymaking issues of the next 20 years. The underlying problem involves advanced machine technologies (i.e., machine learning, natural language processing and sentiment-analysis tech) that will be able to impersonate human speech. Does this technology, designed and maintained by humans, have the right to free speech? So far in the United States, the answer is 'yes' based on challenges to 'speech' such as Google's search results. Can more-advanced technologies designed for speech (e.g., bots) be taken to task for libel and/or harassment?

"Our fundamental freedoms as individuals are beginning to converge with 'smart' technologies, and we'll have to find solutions – both in terms of short-term fixes as well as long term policies – to deal with this problem."

Limiting rights is not likely to reduce the most dangerous fake and misleading information

Some respondents said that there is no way to stop highly motivated actors (whether they be human or bots) from routing around attempts to establish the real identities of all who post misinformation, or to limit, flag or block content.

Tom Rosenstiel, author, director of the American Press Institute, senior non-resident fellow at the Brookings Institution, commented, "I strongly doubt changes can be made in any structural way to reduce fake and misleading information. The platform companies may make some efforts, but those will collide to some degree with other values they have about open communities and to some extent collide with their revenue models, which favor intense engagement. There is a bias there toward strong emotion, both cheering and panicky. In theory, there could be regulatory efforts to blunt this, but in reality there is nothing to suggest any political environment in which such regulations would be enacted. We have been moving away from that now for 40 years, and the signs at the moment point toward that only continuing further. By the time the political system would be ready to address this problem, the problem would have changed. And absent that, the efforts by platform and distribution companies to police their own landscapes will be unable to keep up with those who want to deceive or misuse the web and those efforts will be muted in any case."

A **researcher investigating information systems user behavior** replied, "This is a global problem, and First Amendment rights are seen differently in different parts of the world. Without some kind of high-quality, difficult-to-spoof identification system it's unclear that the amount of misleading information can be reduced."

An **institute director and university professor** said, "If there *was* a way [to reduce fake news], the publishers of the National Enquirer would have been put out of business a long time ago. Instead, they're dining at the White House."

A **vice president for an online information company** was among a number of anonymous respondents to this survey testifying on behalf of the right of some degree of anonymity, "If no one can speak anonymously, unvarnished truths may evaporate and be replaced with falsehood; people may be afraid to say what they think; freedom of expression suffers. On the other hand, unbridled freedom to speak may not solve the problem either because it may become harder and harder to distinguish truth from fiction… Allowing only strongly-attributed speech will drive some truths underground."

Ian O'Byrne, assistant professor at the College of Charleston, replied, "Anonymity, and the ability of individuals and bots to routinely spawn new accounts leads to a system where anyone can say anything while harming the civil liberties of others. Perhaps 'real identities' need to be pursued, while anonymous, or 'off the record' accounts/messages are somehow discredited may help. The end result would then [however] be a discourse system in which everyone is 'real' and verified and a second discourse system where all accounts are fake, unverified, et cetera. This ultimately would lead us back to our current situation."

Some pointed out that most members of the general public have very little chance of remaining anonymous anyway, due to the ways in which their online movements are easily tracked by powerful corporations or governments that database their acts in a way that can create a very recognizable online identity. An **anonymous respondent based in Europe** wrote, "In a networked world, with all the digital government and business services, it might be difficult (if not impossible) to keep the the same level of individual privacy, unless states and societies would grant citizens a choice of alternative of fully or partially 'analogue' living, regardless the economic costs and inconveniences. Most likely the latter is not happening. At the same time, societies need to be cautious of any calls and statements that some rights have to be curtailed."

A **leading internet pioneer who has worked with the FCC, ITU, GE, Sprint and VeriSign commented**, "Privacy is not possible."

A **professor and associate dean** commented, "Our most important tool for the preservation of civil liberties is anonymity, and it is also our most destructive. We need a barrier between anonymity and identification whose porosity can be turned on and off. The legal system can do this: I post something terrible anonymously. A legal action is brought against me to determine who I am and investigate my claims. The courts will need to adjudicate such actions. Imperfect, of course, and likely to jam the courts, of course, but there is a way."

A **senior attorney for a major online civil rights organization** said, "People always want to clamp down on online anonymity whenever online speech gets messy. But anonymity isn't the problem – our very own president repeatedly misleads in public – it's not an attribution problem."

James LaRue, director of the Office for Intellectual Freedom of the American Library Association, commented, "Even unfailingly attaching identity to statement doesn't work to reduce fake and misleading information. We need to incentivize truthfulness. Reward people for civil discourse. Award points for fact-checking, and for withstanding those checks. A second option is legislation, criminalizing some kinds of speech. But that, clearly, is fraught with a host of First Amendment issues."

Others responding about anonymity wrote:
- A **consultant** said, "Anonymity may need to be restrained. Accountability will be required."
- A **vice president** for stakeholder engagement said, "Anonymity on the internet is a concept whose time has passed."
- A **professor and researcher** noted, "To reduce disinformation with current techniques we need to identify the source of every piece of information through the provenance chain to the beginning. There will be no privacy or anonymity in such a society."
- A North American **research scientist** wrote, "We need systems to require more transparency. The right to anonymity will be collateral damage."
- A **public-interest lawyer** based in North America commented, "I don't see a way to do this without dangerous degradation of the First Amendment."
- A self-employed **marketing professional** observed, "1984 would result."
- Ironically, an **anonymous respondent** commented, "I oppose anonymous and/or unattributed responses on the internet. Everyone's participation should be identifiable as theirs."

Some solutions may help limit misinformation while preserving rights to some degree

Susan Etlinger, industry analyst, Altimeter Research, said, "I have to believe that any attempt to reduce misinformation must preserve civil liberties or it is simply a weapon available for use by the highest bidder."

A number of people said there are potential remedies that may at least slightly improve the information environment while minimizing damage to civil liberties.

Bill Woodcock, executive director of the Packet Clearing House, wrote, "The intersection of cryptographic signatures and third-party reputation tracking may provide some relief provided the reputation tracking is neither completely politically co-opted, as is the plan in China, or trivially manipulated by hackers or astroturfers. The combination of PGP and blockchain will probably help a lot. There have been attempts like Diaspora to build a platform on which identities and speech could flourish globally, but I think, unfortunately, the age of Usenet has passed, and commercial speech is trumping both gratis and libre speech."

Jonathan Grudin, principal design researcher, Microsoft, said, "We have always had tremendous quantities of incompatible information, such as conflicting scientific claims or different religions insisting their tenets are true and others false. The solution is to organize the information and its claims and identify its provenance. It will take some time to do this and for people to learn about it. I credit people with the ability to master this."

Alexander Halavais, associate professor of social technologies, Arizona State University, said, "Implicit here is whether changes may be made in government restrictions, and I don't think we want public truth police. Justice Brandeis already answered this for us: 'no danger flowing from speech can be deemed clear and present, unless the incidence of the evil apprehended is so imminent that it may befall before there is opportunity for full discussion. If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence.' Some of that may consist of meta-speech. Certain people have been better and more consistent in telling the truth over time, and I suspect we will find new ways of identifying them. While it may seem to be a problem of 'turtles all the way down,' and certainly efforts to assail the neutrality of, e.g., Snopes suggests that this will be a problem, there are counter-examples in social media – from Wikipedia's NPOV (neutral point of view) efforts to

Slashdot's meta-moderation – that suggest that there are ways of creating the equivalent of the Better Business Bureau for truth claims."

Veronika Valdova, managing partner at Arete-Zoe, noted, "Freedom of speech is not an absolute right. Unprotected speech includes obscenity, child pornography, fighting words and true threats. Particular categories of speech can also be subject to criminal or civil suit, such as disclosure of classified information, the disclosure of personally identifiable health information, defamation, libel or slander. Commercial free speech is yet another topic, fiercely disputed in, e.g., pharmaceutical advertising (see U.S. vs. Caronia). False testimony is not protected either. Impersonation, threats and hate speech and revenge reputation damage including revenge porn are currently difficult to prosecute but that may change. German authorities are taking the protection of their information environment very seriously, due to historical experience with the effect of Nazi propaganda."

The **technology editor for one of the world's most-respected news organizations** commented, "Free speech may have to be curtailed in some specific cases (in Germany Holocaust denial is illegal, for instance)."

Charles Ess, a professor of media studies at the University of Oslo, wrote, "Efforts to reduce fake and misleading information will, among other things, have to severely reduce the possibilities of anonymous communication online: this means a reduction in privacy and at least anonymous forms of free expression. The counterweights to ensure that these restrictions in turn do not become misused by those in power include far more robust educational efforts aimed at helping citizens better understand and develop the basic skills and capacities – the virtues – required for not only effective political discourse online, but also democratic citizenship more broadly. We need nothing less than a new enlightenment, one that sustains classic Enlightenment-Democratic theories and norms, but as transformed as needed for life in a world dominated by digital communication technologies."

Susan Price, lead experience strategist at Firecat Studio, wrote, "Reliable attribution is the way forward; verification of news by a number of trusted sources can be the basis of crowdsourced verification, similar to movements of schools of fish or flocks of birds. Individuals need the ability to closely control the release of information of their own data through a human API, and this could form the basis of a workable compromise between privacy and transparency. Anonymity must be available to protect against fascist control."

Justin Reich, assistant professor of comparative media studies, MIT, noted, "Most forms of fake news are squarely protected under the First Amendment. Social censure will stop fake

news, just like social censure has had some effect in curbing common racist, sexist, homophobic speech without curtailing rights."

Sandro Hawke, technical staff, World Wide Web Consortium, noted, "The only 'rights' that have to be curtailed are the 'rights' to be anonymous and to lie without consequence, which have never been accepted as rights. There is a value to anonymous whistleblowing, but that has to be managed very carefully for the good of society, and should not be seen as a civil right. There is also a value to being able to speak to millions of people at once, but again, that's not a right. Our best approach will be to consider how small groups of humans handle fake and misleading information. In these groups, where everybody knows everybody else, people can hold each other to account for gossip, slander, and swindling. In our headline dive into the internet (and even radio and television, as we relaxed regulation), we left behind many of our tools for managing information quality. It will take some work, but we can (and must) bring them back."

Matt Armstrong, an independent research fellow working with King's College, formerly executive director of the U.S. Advisory Commission on Public Diplomacy, replied, "No rights need to be curtailed. This question pretends we can work around the consumer. The consumer/producer/repeater all must be called out, shown as the agents/naïfs they are. Reducing the demand and success (thus 'profitability') will reduce the fake and misleading information. One tactic is to shame the consumers and repeaters, but it requires education and support by leaders from civil society, including education and politics."

Michael R. Nelson, public policy executive with Cloudflare, replied, "We can definitely preserve civil liberties unless we extend to eliminate all misinformation. Doing that would require eliminating anonymity online in order to deploy effective reputation systems, which would highlight misleading or bogus information. But the end of anonymity would limit free speech, particularly in countries where repressive government censor or arrest journalists or bloggers."

Jim Rutt, research fellow and past chairman of the Santa Fe Institute and former CEO of Network Solutions, replied, "A real name ID policy rigorously enforced is the strongest relatively easy play. Unfortunately, this has some negative impact outside of The West, and perhaps in it as well."

Jennifer Urban, professor of law and director of the Samuelson Law, Technology & Public Policy Clinic at the University of California-Berkeley, said, "We have existing legal models that deal with false information (fraud, defamation) and with other types of harmful

information (e.g., harassment). What we do not yet have is a way to scale these rules to the internet. But if we can develop that, then yes, we can better reduce false information while leaving in place the current protections for civil liberties. We should not assume that we have to curtail civil rights to address this problem. It seems unlikely that curtailing civil rights would work – see every authoritarian regime that struggles with activists' commentary – and there would be a greater loss."

Jerry Michalski, futurist and founder of REX, replied, "We may need stronger identity authentication for people posting information, which will reduce the rights of people who want to remain anonymous. But I think we can find solutions that don't do much more harm than that."

Greg Lloyd, president and co-founder of Traction Software, wrote, "First, reduce economic incentive to spread fake news by pressuring advertisers (social, legal). Some public forums may require authentication to participate – or even read. New regulation based on 'false advertising' principles might work. Individuals' personal rights can be preserved, with existing libel, hate speech, threat, blackmail, et cetera, laws."

Irene Wu, adjunct professor of communications, culture and technology, Georgetown University, said, "We need media leaders in civil society, business and government to provide information on topics they want to hear about in a way that appeals to them in a manner that demonstrates the credibility and validity of the reporting. Maybe it's time to make more explicit the number of sources a journalist is using to write a report – two if on the record (with their credentials), one if off the record, corroborated by statistics from which institution. Can you put a badge on an article that lists these, like a nutrition label on a cereal box? I think the good reporting needs to be highlighted more. Curtailing civil liberties does nothing to improve the quality of public discourse."

Steve McDowell, professor of communication and information at Florida State University, replied, "The tasks and social roles of journalists as trusted reporters and commentators may become more important, in that we might also ask them to provide an assessment of the quality of information or claims and statements in stories. This information about procedures should be provided to the public. If technical means or organizational procedures are adopted by social media sites to filter or block information, these sites should be transparent about how their automated systems or organizational procedures operate. Just as with child protection web-blocking software, there will be over-blocking based on keywords, or underblocking. Software will have ongoing learning capabilities built in, but may be behind human actors with specific agendas."

Filippo Menczer, professor of informatics and computing, Indiana University, noted, "Trusted news standards and their technological implementation and enforcement must strike a balance between free speech and the right not to be deceived. The two can coexist."

Laurel Felt, lecturer at the University of Southern California, wrote, "Through [many] mechanisms… users can choose to receive information about a source's trust rating. In terms of mainstream broadcast news, perhaps a fee can be levied when an organization shares uncredible information."

Susan Hares, a pioneer with the NSFNet and longtime internet engineering strategist, now a consultant, said, "Technology can double-check information. Academic systems already check attributions or plagiarism. Computer systems can highlight plagiarism, quotes that are wrong, incorrect facts and correct details. Civil rights do not have to be curtailed. Websites can choose to not publish erroneous information. Legal suits can be allowed against web sites that publish erroneous information. Individuals can choose to refuse to use websites that provide erroneous information. I currently refuse to watch news channels with a high bias. I do not buy products from companies that sponsor these new channels."

Paul Jones, director of ibiblio.org, University of North Carolina-Chapel Hill, suggested, "Certification of publishers, but not licensing, using technologies such as blockchain, could make brands responsible to the public with out curtailing rights Americans hold dear. Responsibilities should be the focus rather than *only* rights."

Larry Keeley, founder of innovation consultancy Doblin, commented, "Imagine a world where information shared digitally has an embedded bar code, and when you read it, it takes you to the audit data for the information being shared, revealing the total confidence interval and all the sources, each with their audit information and confidence intervals revealed. This happens all the time now for some fields. It is inevitable for the best information systems too."

A **professor of law** at a major California university observed, "We have existing legal models that deal with false information (fraud, defamation) and with other types of harmful information (e.g., harassment). What we do not yet have is a way to scale these rules to the internet. But if we can develop that, then yes, we can better reduce false information while leaving in place the current protections for civil liberties. It would be a bad idea to assume we have to curtail civil rights to address this problem. It seems unlikely that curtailing civil rights would work – see every authoritarian regime that struggles with activists' commentary – and there would be a greater loss."

Tom Birkland, professor of public policy, North Carolina State University, commented, "Some changes in civil law to make it easier to prosecute malicious falsehoods – such as the Pizzagate problem – might cause media companies and producers to more carefully vet their information. And since access to platforms like Facebook and Twitter is not a fundamental right, the owners of these networks should be more responsible for the worst kinds of misinformation that is posted in these services."

A **professor and researcher of American public affairs at a major university** replied, "State pressure on foreign actors can help preempt attacks by bots. And media institutions can cooperate to ensure that fake information doesn't overly influence the tone and coverage of political campaigns."

A **research associate at MIT**, said, "Perhaps libel laws need to be strengthened. Some may view this as curtailing First Amendment rights. However, fraud is distinct from the right to be wrong. That is where law and society need to and will innovate. One more thought: calling an outlet 'fake news' should be considered slander or libel if the person using the phrase knows that the news is not actually fake."

An **author and journalist based in North America** suggested, "Revise the Communications Decency Act and apply libel laws to online communication. The risk of court remedy has always been a good incentive to check your facts before hitting send. If this practice chills the lies, so be it."

Stephen Bounds, information and knowledge management consultant, KnowQuestion, said, "Societies *already* mandate information sharing or withholding in certain circumstances. Sometimes criminal or private information may not be legally shared. In other circumstances, information *must* be disclosed, as when a person has reasonable suspicions of abusive activity or to allow shareholders to make informed investment decisions. These rules are an attempt to ensure justice and fairness for everyone, where there are incentives for people to act in selfish ways. Mostly laws already exist to prohibit the kinds of acts broadly covered by 'fake and misleading information.' The problem is detection and enforcement."

Seth Finkelstein, consulting programmer with Seth Finkelstein Consulting, commented, "Changes can be made to reduce fake and misleading information by massively increasing public funding of academia, nonpartisan expert agencies, holding extensive intellectual events, and so on. For example, there needs to be far more ability to have a financially secure career as a public intellectual, without needing to be an attention-seeking social media

hustler or some sort of corporate propagandist. Just as a starting point, let's have an American implementation of a strong independent and well-funded BBC News, before any thought of curtailing rights. To put it very simply, corporations that make money selling eyeballs to advertisers, don't, as a rule, care much about what goes into getting those eyeballs in front of the advertising. If market values are the only things that matter, the results are going to be dismal."

Internet platforms are seen as a potential help and as a big part of the problem

A **partner in a services and development company** commented, "No rights need to be curtailed, but some rights need to be formulated more clearly and defended more vigourously… Internet intermediaries (especially search engines, social networks and advertising exchanges) will have to limit or stop certain problematic practices and/or support measures that mitigate the loss of freedom suffered by their users."

Evan Selinger, professor of philosophy, Rochester Institute of Technology, wrote, "To comment on but a fraction of what's at stake in this question, the balance between reducing fake information and preserving civil liberties is a contextual issue. In the context of corporate platforms, like Facebook, there are two important things to keep in mind. First, the idea that Facebook is merely a conduit for user-generated communication has outlived its expiration date; it's laughably implausible. Second, normative consequences follow from acknowledging that Facebook's curatorial power is a mechanism of techno-social engineering that affects what people see, believe and think. For starters, since that power is deployed through algorithmic governance, there are good reasons to believe that greater transparency should exist and less weight should be given to the ideal that valuing corporate secrecy requires making black-boxed software sacrosanct."

Marina Gorbis, executive director of the Institute for the Future, said, "What is driving proliferation of misleading and sensationalist information are business models behind the main media channels. Reliance on advertising dollars and the drive to attract 'eyeballs' create a media environment that is not driven by public interest but rather by financial goals. Today Wikipedia, a nonprofit commons-based platform is the most unbiased and well-functioning media outlet we have. There are lessons from Wikipedia in how we need to evolve our media environment."

Brian Harvey, teaching professor emeritus at the University of California-Berkeley, said, "Anonymity is a prerequisite for non-fake news; think Pentagon Papers, Deep Throat, NSA

malware. The only 'right' whose curtailment would help the quality of public information would be the right of accumulation of capital."

An **internet pioneer and principal architect in computing science** replied, "The internet's advertising oligopoly has profited greatly from the distribution of fake news, putting the rest of us at risk. Advertisers have started the counter-revolution by organizing a boycott. We do not need to curtail civil liberties for that boycott to succeed – all we need to do is to make distribution of fake news less profitable."

Jim Warren, an internet pioneer and open-government/open-records/open-meetings advocate, said, "The most crucial 'right' that must be curtailed has been, and will be, restricting how much of the information media can be controlled by one entity (governmental or corporate). We have always had fake and misleading information. Its only redress is to assure that others have equivalent opportunities to respond in timely and robust ways, to more or less the same audience."

Jason Hong, associate professor, School of Computer Science, Carnegie Mellon University, said, "Facebook and Google have the biggest role to play here because they not only make it easier to find misinformation, but also (inadvertently) help incentivize it through ad payments and clicks. As the old saying goes, follow the money. While this won't stop state-based actors, cutting of advertising revenues for egregious sources of misinformation would severely undercut incentives for a non-trivial portion of fake news. The challenge, of course, is how to draw clear lines as to what is and isn't fake, and to have a fair process that doesn't harm potentially legitimate sources of information."

A **professor of sociology based in North America** said, "Powerful media companies can help filter valid content. If trust is restored to news sources, I don't expect personal liberties to suffer as a result. Social media will continue to allow people to share ideas, whether true or false."

Constance Kampf, a researcher in computer science and mathematics, said, "People need to be continually developing their knowledge, and fake and misleading information are a challenge that we need civil society to overcome. No technology can think for us, and no platform can replace critically engaged citizens. That said, a look into the fourth estate and the state of journalism today, as well as the dominance of Google and YouTube as search engines that deliver information and use algorithms that affect access to information, does call for rethinking. I think Google's right to experiment with algorithms affecting access to internet information should be publically and critically examined with its' role in directing

the publics' attention. Is it appropriate for these algorithms to be privately controlled? So tech companies rights should be examined, but freedom of speech for individuals should remain a priority – with the same level of responsibility that the U.S. legal system currently gives for slander and endangerment."

Henning Schulzrinne, professor and chief technology officer for Columbia University, said, "Private platforms can strengthen the ability to determine the source and their trustworthiness, e.g., by scoring their lifetime factual truth average. Best practices for corrections and challenges, similar to the security responsible disclosures model, may work. There might be a way to tie this to campaign finance reform, to the extent that the candidate solicits or pays for fake news."

Ian Peter, internet pioneer, historian and activist, observed, "There is an assumption here that the spread of information via social media could somehow be curtailed or controlled. But when things go viral, many people unwittingly contribute to the spread of fake news. Add to this the use of 'bubbles' and algorithmic feeds that send you what algorithms suggest you might want to believe; you then have a messy situation. No laws ever stopped gossip, and no laws are likely to curtail fake news."

A **technical evangelist based in Southern California** said, "The best we can do is to flag/annotate possible problems with issues/reasons, not filter."

A **professor and expert in technology law at a West Coast-based U.S. university** said, "No, there is no way to avoid [infringement of civil liberties]. Intermediaries will figure this out, consistent with rights to free speech and press."

But a **fellow with an international privacy rights organization** disagreed, saying, "I don't believe the solution to the problem of fake news is through censorship, specifically automated censorship through the use of opaque algorithms [by platform companies like Facebook and Google]. That is because those solutions only get us closer to a 'thought police' and a curtailing of freedom of expression and privacy online. Instead we must realise that the problem will not be solved through technological means, as it is not a technological problem."

A **North American research scientist** observed, "I for one don't want Facebook deciding what's true. I can already hear the screams of 'censorship!' That's where we are heading if we want systems to think for us."

A **professor and researcher based in North America** noted, "Yes. I don't know why civil liberties would need to be curtailed. Most of the misinformation I see is circulated by exploiting the affordances of social media systems with the tacit support of private industry. For-profit corporations such as platform providers should be regulated and held accountable but the free-speech rights of individuals need not be curtailed."

A **senior international communications advisor** commented, "We might want to develop something along the lines of 'truth in advertising' model and then legislate that all Google, search engines, be accountable for what they distribute. The historical record tells us that consent is often manufactured – including consent for repression. The most effective form of brainwashing is through mass media."

An **editor and translator** commented, "All the systems and measures to prevent misinformation will be used by corporations and governments to suppress any type of undesired voices. Even now anti-hate speech measures of major social media platforms are mainly used to remove content by certain minorities or dissidents. Freedom of expression, right to information are the first rights to go."

Jonathan Brewer, consulting engineer for Telco2, commented, "Any changes in social media platforms attempting to reduce fake and/or misleading information will only be as effective as local markets allow them to be."

An adjunct **senior lecturer in computing** said, "Most rights have been curtailed but not by enforcement. The young likely to protest have been diverted by social media pulp. Older dissidents protest through social media but are drowned out by the 'buzz' of inconsequential pulp. Any popular movement that has significant general exposure in the media is soon forgotten, replaced by something horrible occurring around the world."

A **distinguished engineer for a major provider of IT solutions and hardware** commented, "This is the crux of the problem: It is not possible to censor sources or articles of news without fundamentally infringing on the right to freedom of expression. My truth may not match yours, but that doesn't mean it is wrong… Human senses are imperfect, and what I perceive when looking at something may be very different from what you perceive. That doesn't make either of us wrong."

Jeff Jarvis, professor at the City University of New York Graduate School of Journalism, commented, "Free speech includes the right to edit, to chose what one shares. So I see no threat to the civil right of free speech in encouraging both publishers and platforms to

account for – as Google has said – reliability, authority and quality in their ranking and distribution of information and content. I see no problem in discouraging advertisers from financially supporting misinformation and fraud. And I see no problem in encouraging the public to share responsibly."

John Wilbanks, chief commons officer, Sage Bionetworks, replied, "It's unwise to conflate how private companies monetize speech with 'the public sphere.'"

Create resilience and embed critical thinking rather than 'trying to destroy all lies'

Patricia Aufderheide, professor of communications, American University, said, "The basic problems are not at the level of the utterance itself but all the political, diplomatic, regulatory and commercial incentives to mislead."

Many respondents urged that each individual must be encouraged and educated in such a way that they become responsible for that which they create, share and take to be "truth."

Serge Marelli, an IT professional who works on and with the Net, shared a few rights that might be curtailed, writing, "The right to lie to oneself, the right to be stupid. The right to (choose to) keep believing in something/anything false *despite facts*. The right to believe in 'alternate facts,' The right to believe in 'creationism.' The right to mix-up fiction and reality."

Esther Dyson, a former journalist and founding chair at ICANN, now a technology entrepreneur, nonprofit founder and philanthropist, expert, commented, "The most important is effective education for all. Create resilience to lies rather than trying to destroy all lies."

Wendy Seltzer, strategy lead and counsel for the World Wide Web Consortium, replied, "We can change how we react to information. That – over the long term – can change how misinformation spreads."

Alejandro Pisanty, a professor at UNAM, the National University of Mexico, and longtime internet policy leader, observed, "A new social compact has to be arrived at; not being lied to has to become a right on a par with all others. Curtailing rights will not work. A better-educated society is the only way 'good' actors may force 'bad' actors to limit their malfeasance."

J. Nathan Matias, a postdoctoral researcher at Princeton University, previously a visiting scholar at MIT Center for Civic Media, said, "The most powerful, enduring ways to limit misinformation expand the use of civil liberties by growing our collective capacities for understanding. In my research with large news-discussion communities for example, encouraging people toward critical thinking and fact-checking reduced the human and algorithmic spread of articles from unreliable sources."

An **internet pioneer and rights activist based in the Asia/Pacific region** said, "There should be quality control before launching services and apps, and due-diligence reviews about possible effects both positive and negative. Of course unexpected effects will most likely happen, but at the moment there are way too many services and applications that are launched without any consideration about what their impact might be. No rights will have to be curtailed. It is about education and being responsible internet users as well as being responsible content producers, apply investigative journalism best practices."

Bob Frankston, internet pioneer and software innovator, said, "We need to make critical thinking an essential part of our culture, push back on our worship of 'winners' and get a better understanding of the importance of external factors (luck)."

Pamela Rutledge, director of the Media Psychology Research Center, urged, "We have to arm people with media literacy and the technological skills to navigate the digital world and overcome fear of information systems. People give away freedom when afraid. Once given away, it's hard to get back."

Richard Jones, a self-employed business owner based in Europe, said, "Selective out-of-context information is embedded in human nature to manipulate. It is not new... The idea of privately sieving ideas before publicising them has not been adopted in the behaviour of many young. And amongst all groups instant communication is used to attempt to recruit for causes or disseminate propaganda. Awareness needs to be improved, gullibility reduced. Religious and political texts have always sought to conscript people's minds. The Gideons placed Bibles in hotels, Jehovah's Witnesses knocked on doors, the end of the world was announced on sandwichboards on Oxford Street. The difference is in volume, accessibility and gullibility."

An **anonymous research scientist based in North America** wrote, "The solution is not to curb information, instead it's to create a stronger democracy in which our bonds to each other do not rely solely on fragmented information communities but a stronger civic infrastructure that has relational bonds that counteract the power of online misinformation."

A **graduate researcher at Northwestern University** wrote, "We can preserve civil liberties if we improve education around these issues, because that will enable community-based regulation of online spaces."

Paul Gardner-Stephen, senior lecturer, College of Science & Engineering, Flinders University, commented, "Perhaps the most effective measure would be to encourage critical thinking among the population, and reversing the anti-science movements that have fostered the hyper-subjectivism that has allowed fake news to flourish. In practical terms: The more educated the population, the harder they are to dupe. Legislative measures, such as that recently taken by Germany to penalise social media platforms for failure to remove obviously fake news will help somewhat, but are only short-term solutions, and form part of the arms race. The main advantages in the long term are to remove cost and other barriers to improving educational attainment and finding ways to achieve de-escalation of partisanism in democracies that have led to these naked attempts to maintain power at all costs, rather than the entire political spectrum in these nations accepting that periods in opposition is a normal and healthy part of democracy."

A **chief executive officer for a research consultancy** said, "A Google search 10 years ago turned up original documents, today it is almost impossible to peel the layers away. The flood of information has dumbed down the ability to learn or even see new things. When society is more curious and active for a better future and more engaging social contract, then what's shared will be more powerful. Unfortunately this starts at the top of the political spectrum."

Hjalmar Gislason, vice president of data for Qlik, noted, "Educating people on information literacy and facilitating systems that help rate or rank the accuracy of information found online is more important. In other words: People should have the right to publish nonsense, but other people should also have available to them tools to understand the veracity of information they come across."

Geoff Scott, CEO of Hackerati, commented, "Fake and misleading information is being used to degrade civil liberties. The only way to reduce fake and misleading information and restore civil liberties is to ensure that the vast majority of people do not believe it."

Deirdre Williams, retired internet activist, replied, "Fake and misleading information is powerful because of the current capability, provided by communications technology, for it to propagate. The solution, if any, depends on re-creating human trust and human trust

networks, and the loss of the 'lazy right' to consider that the headline from a 'reliable' source is the truth, without trying to do any supporting research."

Paul Saffo, longtime Silicon Valley-based technology forecaster, commented, "This has always been a balancing act and the future will be no different. Recall (U.S. Supreme Court Justice) Oliver Wendell Holme's famous dictum about shouting 'fire' in a crowded theater. This time we are balancing on a digital razor's edge, where acts that are innocuous in the physical world have outsized consequences in cyberspace. We all need to remember that with rights come responsibilities, and the more potent the right, the greater the burden to behave responsibly."

Bryan Alexander, futurist and president of Bryan Alexander Consulting, replied, "We can reduce the influence of fake news by teaching digital literacy to individuals, so that they can make better decisions."

Charlie Firestone, executive director, Aspen Institute Communications and Society Program, commented, "Free societies have always faced fake or false information. Actions such as curtailing advertising to such statements and increased media literacy should help in bringing about the desired result without curtailing liberties."

Adrian Schofield, an applied research manager based in Africa, commented, "The notion of civil liberties is false. No one person can have rights because they come at the expense of another person's rights. There should be no rights, only responsibilities. If each one of use can be held accountable for our own behaviour, there will be no victims. The passive majority lives in this fashion."

David J. Krieger, director of the Institute for Communication & Leadership, Lucerne, Switzerland, commented, "We must move away from ideas of privacy as secrecy, anonymity and disguise and create trust-based networks in order to maintain freedom, autonomy and human dignity in the digital age."

Riel Miller, an international civil servant who works as team leader in futures literacy for UNESCO, commented, "If a sucker is born every minute does that mean a warning label needs to be smacked on the false goods every minute? Challenge is to equip the user; they must learn to fish."

The information explosion is so overwhelming we need to rethink things

A **researcher at a European institute of tecnology** replied, "Controlling information doesn´t appear as a promising solution. Instead we need to find strategies to cope with the new situation in a way that is compatible with our understanding of society (including the preservation of civil liberties). In the first place this means that the society needs to be educated, especially with regard to media literacy and critical thinking. However, very negative behavior should indeed be sanctioned without touching free speech too much (e.g., calls to harm human beings should be punished)."

A **futurist based in North America** said, "It is unrealistic to think that fake and misleading information can be reduced. A new civil contract might help, but it is unlikely that uninformed/misled citizens will be cooperating in generating reliable information. Most of them just prefer sensational information – real or not."

A **professor of media and communication based in Europe** said, "Each digital society has to rearticulate its civil liberties in the face of new technologies; such recalibration requires a systematic rearticulation of legal frameworks that currently are not prepared for algorithmic-based clashes of values and norms."

Barry Chudakov, founder and principal, Sertain Research and StreamFuzion Corp., wrote, "We now need an Information Bill of Rights with international signatories. We need to take into account the ubiquity of personal information and tracking; we need to institutionalize information watchdogs who will review collection and revelation standards from both programmed AI and live captures. We are in a new world and we need new-world tools and standards to establish protocols and protections. Included in the Information Bill of Rights should be such protections as: freedom of the press' sources named and unnamed; the right to both protect and disseminate information for the public good; the right to know who is collecting data on you, or anyone, and the right to see all levels of that data – to name a few. The democratization of data brings with it the responsibility to establish widely adopted governance protocols.

"According to EMC: 'By 2020 [the digital universe will contain] nearly as many digital bits as there are stars in the universe. It is doubling in size every two years, and by 2020 the digital universe – the data we create and copy annually – will reach 44 zettabytes, or 44 trillion gigabytes.' While these sums are mind-boggling, even more boggling is that we are letting this information ship go without steering, without a rudder. We can preserve civil liberties

once we establish a set of standards for collection, transparency, transmission and other key issues… We have taken a *laissez faire* attitude to one of the most powerful forces ever unleashed by humans: exponentially multiplying information and information collection and manipulation systems.

"Once we have formulated – and there is broad adoption of – an Information Bill of Rights, the next step to reduce fake and misleading information is to educate as well as inform. Free citizens in the new information environment have a unique imperative: we all must be information omnivores because we now see clearly that information does not have a neutral intent; bad actors are using misinformation to effect their agendas. Just as we educate children about personal hygiene and proper nutrition, from an early age, we must teach our children – and then insist on adults in positions of authority – that they balance information sources and facts from a broad stream of media. Narrowcasting is the enemy of freedom. Broadcasting, and broad thinking, will preserve democratic perspectives and voices."

A selection of additional comments by anonymous respondents:
- "Civil liberties, especially First Amendment rights, are the most threatened."
- "Economic incentives for fake and misleading information have to be curtailed."
- "If it was 35 years ago and we prohibited corporations from profiting via news as entertainment, we would be in a less sensationalist, ad-driven situation."
- "Whatever we develop to ameliorate a problem can and will be turned against us. I have no problem with labeling, with debunking, with doing our best to maintain standards, but the emphasis should be on critical assessment and media literacy, not prohibition."
- "Data is raw. How people tailor, shape and use it will be never-ending. Teaching people digital literacies and cognitive thinking will be the only way to sort through data inputs… There is no success to be found in panopticons."
- "Fines for flat-out lies? Would that work?… But ideological 'truth' or spin or perspective or interpretation – who would determine that?"
- "Democracies endeavour to allow free speech but in practice find they have to set some limits on advocates of violence."
- "Fake news is being used to advance an agenda of reduction of free speech."
- "The only real 'thing' that can be done is to eliminate monopolies of information and stop the collection of personal data, much like we once stopped monopolies of rail."
- "Driving propaganda out of our society is best undertaken not by attacking 'fake news' directly but by decreasing the susceptibility of everyday people to hyperbole, lies and innuendo."
- "Identify a rating system for reports, writers and media outlets."

- "A stronger focus on election reform and good governance would reduce a lot of the motivations to spread harmful information, without harming civil liberties."
- "It has to be social pressure and not law that demands better information. People must care about being emotionally hijacked by misleading information."
- "Ha! We have no rights if we are using a private service like Facebook or Twitter. They can do whatever they want."
- "Users' browsers will give them warnings when the source of information cannot be validated."
- "The danger to undoing civil liberties is in thinking that by restricting them we are someone going to make the world a safer and trustworthy place."
- "Education systems should be designed so students get authentic experience in rational decision making and seeking out a multitude of voices on any issue. The cultural norm of being a good thinker needs to be reestablished."

Follow-up #4:
What do you think the penalties should be for those who are found to have created or knowingly spread false information with the intent of causing harmful effects? What role, if any, should government play in taking steps to prevent the distribution of false information?

Most of the respondents who said some sort of action should be taken against those who can clearly be identified as disseminators of disinformation with harmful impact generally pointed out that current laws and regulatory structures can be applied or adapted and applied. Some said corporate actors who have been profiting from such information should be required to step up. Some said it all comes down to acts by individuals, adding that education in information literacy, ethics and morals should be bolstered considerably. And many said there are too many complexities, including cross-border issues and the difficulty of defining who commited an act, what is punishable and why and who gets to decide who gets punished and how.

danah boyd, principal researcher, Microsoft Research and founder, Data & Society, wrote, "What kinds of harm? Which governments? What's at stake is far more complex than is implied here. We're talking about jokesters engaging in similar practices as nation-states, profiteers using the same techniques as ideologues. For example, all governments are

engaged in these practices and one could argue that their information operations practices are harmful."

Susan Etlinger, industry analyst, Altimeter Research, said, "It depends on the context. Are we talking about antibiotics? Children's toys? Or taking down a government? There already are guardrails in effect in many countries to protect the integrity of products, services and institutions. I don't believe we need to reinvent all of those institutions. Rather, organizations that protect public health – food and drugs, and the electoral process, among others – need to account for and guard against their specific vulnerabilities to misinformation."

Micah Altman, director of research for the Program on Information Science at MIT, commented, "The government should be supporting an independent media, and robust information systems that are open, transparent and traceable to evidence and not focused on suppressing false information."

Seth Finkelstein, consulting programmer with Seth Finkelstein Consulting, commented, "[There is] a system of institutional incentives that promotes profitable misinformation over unprofitable but true information. The following sentence encapsulates the problem: There needs to be a business model for truth. I'm reminded of the legend, which is completely untrue, that Fox News is supposedly banned in Canada because ‘it's illegal in Canada to lie on airwaves.' Are those proposing penalties for having ‘created or knowingly spread false information' willing to apply them to a large amount of lobbying, campaigning, and, sadly days these days, many media organizations? If so, there are major problems, not the least that such a proposal would go against much of the legal protection for freedom of speech in the Western world. If it's proposed to apply narrowly, then by definition it's only making a few fringe players miserable. Consider Tom Paxton's 1964 song ‘Daily News': ‘Don't try to make me change my mind with facts / To hell with the graduated income tax / How do I know? / I read it in the Daily News.' It's tempting to dismiss the problem as always with us. But it's also distracting to focus only on scapegoat outliers who are safely removed from positions of power."

Marc Rotenberg, president, Electronic Privacy Information Center, wrote, "As the problems are structural, the remedies must also be structural."

Bernie Hogan, senior research fellow, University of Oxford, noted, "The government (here presumably we refer to the U.S. government) should reinstitute the Fairness Doctrine if nothing else. Penalties for misleading information framed as facts will almost always be defended as a first amendment right. This is one area where the Supreme Court seems to

have consistent consensus. Who really needs to step up is platforms. They ought to be less acquiescent to fringe users. However, they appear to be committed to appeasing all their users (from whom they make money). Thus we see here the logic of capitalism reinforcing a profit motive above facts, something I assume will continue to accelerate as the few become more effective at personalising what they curate for the many."

Joanna Bryson, associate professor and reader at University of Bath and affiliate with the Center for Information Technology Policy at Princeton University, said, "This should be treated exactly the same as any other equivalent level of destruction (blowing up buildings, writing on walls). We need to get better at quantifying the damage – a project for economics."

Adrian Schofield, an applied research manager based in Africa, commented, "Most communities have laws prohibiting libel and slander. The challenge is enforcing them. Successful prosecution should result in depriving the guilty party of access to the mechanisms of publication."

Jonathan Grudin, principal design researcher, Microsoft, said, "Ideally the government should distribute accurate information and help establish the provenance of misinformation. It is difficult to prove 'intent of causing harmful effects.' If I lie to elect a candidate I believe will be good, did I intend to cause harmful effects? Where intention to harm can be proven, remedies often exist."

Esther Dyson, a former journalist and founding chair at ICANN, now a technology entrepreneur, said, "There should be some application of legal penalties, but very carefully. The government should run the courts; the people should file lawsuits. There is also a regulatory role for the Federal Trade Commission and the like."

Christian H. Huitema, past president of the Internet Architecture Board, commented, "I would not like to have to write such laws."

Sandro Hawke, technical staff, World Wide Web Consortium, noted, "I don't know exactly why the existing rules concerning fraud and libel are failing us. It might be about anonymity. It might be about jurisdictional boundaries. It might be lack of training for law enforcement. It might just be society is reeling, trying to adapt to a new set of problems. I doubt we need more-severe penalties. We probably need to look at making traditional consequences still enforceable, even with the new technologies. Most of the time, it shouldn't need to rise to the level of law enforcement, though."

Corporate actors profiting from information platforms
should assist in improving the information environment

Jennifer Urban, professor of law and director of the Samuelson Law, Technology & Public Policy Clinic at the University of California Berkeley, wrote, "We already have laws against fraud, defamation, harassment, etc. Those are good models; we need to find a way to scale them. Government's role should be to pressure other state actors that support or engage in spreading misinformation, to enforce the law, and to avoid spreading misinformation itself. We could also consider reviving the Fairness Doctrine, which would require that multiple viewpoints be presented, though this only applied to broadcast license holders. Beyond measures like these lies a very slippery slope towards government censorship. We should also ask about the role of corporate actors – it is Google, Facebook, Twitter, etc., that actually make many of the relevant decisions today."

The **president of a consultancy** observed, "The tech companies who made millions on fake news by ignoring it should be held accountable. Government is so far behind on everything digital, their role has to first be to educate all government employees, then the citizenry, and sustain updates as diverse new false news strategies are identified."

An **assistant professor at a university in the U.S. Midwest** wrote, "If a socio-technical solution is used to address this there can simply be in-system impacts. A person can be flagged in some way depending on the severity of the issue."

Mark Bunting, visiting academic at Oxford Internet Institute, a senior digital strategy and public policy advisor with 16 years' experience at the BBC, Ofcom and as a digital consultant, wrote, "The role of government is to ensure that the intermediaries who operate our information environments do so responsibly, in a way that takes appropriate account of the competing interests they must balance, that provides opportunities for appeal and redress, that is driven by consumers' and citizens' rather than purely commercial interests. It is not governments' job to try to specify in micro-detail what content should and shouldn't be allowed."

Jeff Johnson, professor of computer science, University of San Francisco, replied, "Penalties for that should be loss of account with whatever online service was used to spread the misinformation."

A **consultant based in North America** commented, "The better approaches are economic (pressing the platform companies to bar the worst offenders from access to

advertising revenue) and media literacy. The answer to debates about restricting speech in America has always been that the first and best response should be more speech."

A **post-doctoral fellow at a center for governance and innovation** replied, "Jail time and civil damages should be applied where injuries are proven. Strictly regulate non-traditional media especially social media."

A **journalist who writes about science and technology** said, "The government should sue fraudsters, much the way the FTC currently sues businesses that make false claims or violate laws."

Nigel Cameron, technology and futures editor at UnHerd.com and president of the Center for Policy on Emerging Technologies, said, "Governments should have no role, and false and misleading speech needs to remain free. But, for example, websites/social media companies have their own free speech rights and can excise/label as they choose."

Larry Diamond, senior fellow at the Hoover Institution and FSI, Stanford University, observed, "Digital platforms should take the lead in denying access or demoting in visibility sources that persistently, knowingly, and harmfully distribute demonstrably false information. Government intervention should be a last resort only when there is imminent threat to public safety."

An **associate professor at a major university in Italy** wrote, "Platforms should reduce the circulation of these false information."

A **fellow who works at a university in the UK** said, "I am concerned with how the narrow economic interests that subtly shape the information landscape are being obfuscated by technologies which are claimed to be objective and impartial but really aren't (AI/machine learning, predictive analytics and the like)."

An anonymous **consultant** noted, "The government should follow the money and hold advertisers accountable for paying to be on websites that are spreading disinformation."

An anonymous **futurist/consultant** said, "Rather than government intervention, platforms like Reddit and others should work with their user base to establish rules around the spread of harmful and misleading information."

Andrea Matwyshyn, a professor of law at Northeastern University who researches innovation and law, particularly information security, observed, "The nature of the information matters. That said, if the action violates the terms of use of the platform/social media site, this type of contract breach provides basis for shutting down the user's account, in the discretion of the platform/site. Government should ensure that the information it provides to the public is itself fully accurate."

Stephen Bounds, information and knowledge management consultant, KnowQuestion, noted, "I would support the establishment of on-the-spot fines for certain classes of information infractions. In a similar manner to speeding fines, grossly defamatory or insulting speech could be subject to an on-the-spot fine by a suitably constituted law enforcement body. Given the massive cultural change this would involve, I would recommend a graduated approach with either warnings or points used to encourage behavioural modification without immediate financial penalty. This could be used separately or in conjunction with 'disclose or remove' laws, where a person responsible for a post could be compelled to modify it to identify themselves and any financial incentives received in relation to that speech, or to remove it from publication. Both approaches encourage personal responsibility to the circulation of socially inappropriate information without outright censorship. The complications of anonymous speech are not insurmountable, since the most problematic free speech exists on highly trafficked platforms where there is a clear corporate body to engage with for assistance in enforcement of notifications and user identification."

Amber Case, research fellow at Harvard Berkman Klein Center for Internet & Society, replied, "Governmental regulations might not be able to fully curtail the spread of fake news, as it relies on the emotional impulses of consumers. However, reducing payment incentives through advertising revenue could curtail the spread of fake news. Forcing a pause before spreading or reacting to content could also help. If an individual is found to spread false information and can be identified, then perhaps their ability to post and make revenue could be taken away, but this will not prevent them from operating anonymously. Some education for consumers could help, but this is not a problem that one government can solve. There are many nations and locations at play here, and there is not a 'one size fits all' punishment or law that could be enacted to curtail behavior. It could be made less convenient or profitable for the original poster, or the social networks in question could send a follow up note to all who reposted or reacted to the message with a note that the message in question is fake news, educating the recipient and amplifier on why it was fake news. That way each piece of fake news shared could become an educational moment."

**Individuals and cultures must do a better job
of policing themselves; it is best to generally
avoid any sort of added regulatory apparatus**

Vian Bakir, professor in political communication and journalism, Bangor University, Wales, commented, "It is difficult to establish intent to cause harm at the level of individual people. Probably better to educate people to be suspicious of false information and know where to go to for trusted information."

Alexios Mantzarlis, director of the International Fact-Checking Network based at Poynter Institute for Media Studies, commented, "I would be very very very wary of restrictive government intervention in this space. The media, tech companies, schools and the public all have a lot do before we hand this over to governments. Governments should for the moment limit themselves to educational initiatives and encourage research/debate on this topic."

J. Nathan Matias, a postdoctoral researcher at Princeton University, previously a visiting scholar at MIT Center for Civic Media, wrote, "The most powerful, enduring ways to limit misinformation and expand the use of civil liberties is by growing our collective capacities for understanding. In my research with large news-discussion communities for example, encouraging people toward critical thinking and fact-checking reduced the human and algorithmic spread of articles from unreliable sources."

An anonymous **principal technology architect and author** replied, "We should not have penalties based on intent – the idea that there should be penalties based on intent is a major part of the problem right now. This is one step in the destruction of freedom."

An **author/editor/journalist** wrote, "To attempt to punish after the fact is pointless. Herd immunity to misinformation is far more effective."

Jeff Jarvis, professor at the City University of New York Graduate School of Journalism, commented, "The First Amendment protects the right to lie and to be wrong. Government should play *no* role in controlling public speech. The only penalty for knowingly spreading false information should be shame – which is why we need encourage citizens to adapt their social norms to reward civility over incivility."

A **senior vice president of communications** said, "We don't care about shame any more, and that used to be enough."

An anonymous **journalist** observed, "Overall, we need to equip people to critically evaluate information better through our education systems. We need to create more awareness, and more informed citizens, and there will be need for new legislation in areas such as algorithmic manipulation, but I don't see how one single measure can solve this issue."

Siva Vaidhyanathan, professor of media studies and director of the Center for Media and Citizenship, University of Virginia, wrote, "We used to have such penalties: Social shaming; loss of credibility and status; exclusion from the public sphere. Government should play no role in such dynamics, but government plays an important role in certifying the dependability of much scientific, economic and demographic claims. That should be defended and maintained."

An **associate professor at a U.S. university** wrote, "Communities and journalistic organizations have to develop their own clear standards and educate the public on how to consume information and why they should care about they way they consume that information."

A **professor at a university in Australia** replied, "One idea is for government to financially support investigative journalism and relevant research dissemination, with grants and other funding opportunities. Now that the business model supporting independent high-quality journalism is failing, it may need the support of public entities to continue its vital role as the Fourth Estate."

Edward Kozel, an entrepreneur and investor, replied, "Only changes to social behaviour will/can address the dire situation: any such changes will require a degree of social judgment or even shame (i.e., morality). A difficult subject for government indeed, but changes to our educational system (comprehensive) that include and are embraced by society can bring about such societal changes."

Alejandro Pisanty, a professor at UNAM, the National University of Mexico, and longtime internet policy leader, observed, "The first and most important role of government in this respect is to promote education and support spaces for open, healthy, civil debate. Basics as mandatory vaccinations and science and logic in schools have to be provided as an infrastructure of trust. Unequivocal support for science, and the prosecution of bad actors such as phony medical treatment providers will help keep false information in check. That is, the action is on all fronts, not only on the news front."

Justin Reich, assistant professor of comparative media studies, MIT, noted, "The primary role of local government is developing school systems where students learn the information literacy skills needed to identify or verify fake news. The role of state and national governments will be to support curriculum development and research towards these ends. Sam Wineberg and colleagues at the Stanford History Education Group are doing important work towards these ends."

Michael Marien, senior principal, The Security & Sustainability Guide and former editor of The Future Survey, wrote, "'Crap detecting' should be a major concern for education at all levels. And what about the pussycat press: why aren't they demanding evidence for questionable assertions and examples of so-called 'fake news?'"

Michael R. Nelson, public policy executive with Cloudflare, replied, "Governments can encourage self-regulation like the codes of ethics that have guided journalists for more than 100 years. Attempts to 'make the Internet safe and orderly,' like the July 2017 German law on hate speech and 'dangerous speech,' are overly broad and would certainly be unconstitutional in the U.S."

Andreas Birkbak, assistant professor, Aalborg University, Copenhagen, said, "Governments should use carrot more than stick and try to cultivate a culture that cares about facts without expecting facts to be universal truth."

Ray Schroeder, associate vice chancellor for online learning, University of Illinois-Springfield, replied, "We may need to interpret the libel and slander rules to include knowingly disseminating false information with the intent to wrongfully influence political and policy decision making for personal gain or profit. Media may choose to focus reporting on statements delivered through legislative venues in which contempt proceedings can be initiated for knowingly false and misleading statements."

Jamais Cascio, distinguished fellow at the Institute for the Future, noted, "The penalties should be essentially a 'scarlet letter' – a tag or flag or some kind of transparent labeling that identifies the person as an intentional purveyor of falsehoods. Government would likely have to play a role in universalizing a system, but you'd likely have multiple alternative bodies putting out tagging guidelines. A 'scarlet letter' of sorts identifies the perpetrators as purveyors of dangerous and false facts to any who might interact with them, along with cultural norms that shame the perpetrators, even if they are ideologically friendly."

Serge Marelli, an IT professional who works on and with the Net, wrote, "They should be sentenced to prison for a limited time and be forced to publicly retract and correct any lies. Also, they should be barred from running for public offices. Nowadays, they get elected to be president."

George Siemens, professor at LINK Research Lab at the University of Texas-Arlington, commented, "Penalties should be social, not government-mandated. For example, there are libel laws, but most gossip isn't handled through that legal model. Most is social awareness in networks that results in a softer pressure."

John Laprise, consultant with the Association of Internet Users, wrote, "There will be reputational harm, there should be no civil/criminal penalties."

Dean Willis, consultant for Softarmor Systems, commented, "I'm in favor of exposure and ridicule. You know, like they did to Darwin after he launched that ridiculous theory. Oh wait, he was right."

Governments should not be allowed to take any sort of oversight role

An anonymous **research scientist** replied, "Penalties would require a government 'Bureau of Truth' to determine the 'true' story. Such a bureau would be inherently repressive and even more dangerous than the unrestricted spread of false information. It would resemble the situation in the Soviet Union at its worst."

A **researcher based at MIT**, said, "The government should provide the judicial system that decides these cases. It should not attempt to become the prosecutor of truth."

Garth Graham, an advocate for community-owned broadband with Telecommunities Canada, said, "Since the governors (i.e., external authority), are primary users of public relations manipulation, giving them a role in regulating distribution, is like giving the insane the control of the asylum."

Mark Lemley, professor of law, Stanford University, observed, "While false facts that injure people (inaccurate drug ingredient information, say) can and should be punished, the government should not be in the business of punishing fake news."

Alexis Rachel, user researcher and consultant, said, "There needs to be a cultural shift wherein spreading of false news is looked on as a heinous and dangerous act, versus the current ambivalence. I'm not sure what the government can or should do with regard to this, except lead by example."

An **anonymous respondent** said, "I do not believe we can trust one group to accurately police truth."

A **media networking consultant** noted, "The government's only role is to provide reliable information to the press. Failure to do so should be prosecuted."

A **journalism professor and author of a book on news** commented, "Government role? Yikes! There should not be any government role – otherwise we are China. Letting whatever current regime is in the White House control what constitutes truth and which can prevent the distribution of information that does not support its truth – that would truly end the American dream."

Jon Lebkowsky, web consultant/developer, author and activist, commented, "This question suggests a slippery slope we might want to avoid. The one thing the government has done before and might do again is a 'fairness doctrine.' However involving the government in managing information accuracy or quality invites the potentially greater problem of censorship."

Barry Parr, owner of Media Savvy, replied, "There's no way to do this without limiting free inquiry and dissent. Government action would be disastrous to democracy."

Joseph Turow, professor of communication, University of Pennsylvania, commented, "If such penalties were created and enforced many public relations executives would arguably be liable to prosecution. And the notion that government officials would lord over decisions about the facticity of news often about them or the parties is laced with conflicts of interest and threats to democracy."

Jack Park, CEO, TopicQuests Foundation, noted, "Penalties should fit the nature of the measured harm. Government playing roles in this context raises issues like: who gets to decide what is and is not "false" information? In my view, if there is a role, it should be that the government funds, in the same way it funds biomedical research, ways in which to increase public engagement in civic activities, some of which include crowd-sourced, role-playing-game-based global sensemaking."

Brian Harvey, teaching professor emeritus at the University of California-Berkeley, said, "Throughout history, governments have been among the most prolific creators of fake news. If I could choose between eliminating Breitbart and eliminating the CIA, I'd definitely choose the latter. Not only does the CIA have a bigger budget, but they are better at creating plausible misinformation. When people believe things like that pizza parlor story last year, the biggest problem is not the story itself, but rather the social conditions that leave people so (rightly) mistrustful of social institutions that they find the story plausible. Trump wasn't elected by Breitbart; he was elected by the 2008 bank crash and the government's response to it."

Johanna Drucker, professor of information studies, University of California-Los Angeles, commented, "We have methods of meting out punishment for lying in financial, legal and medical realms (or used to, they are being quickly stripped away). Why not create similar laws and liability statutes for information? My concern about government controls comes from observation of current trends in the Trump administration to control discourse through intimidation, closed briefings, strategic release of misinformation as if it were official - or as official - statements. The checks and balances built into the relationships among the judicial, legislative, and administrative branches of American government are still essential. No single branch should have any exclusive powers over information or it will lead to abuse (of those powers and of information)."

Some type of regulation should be applied, updated or adapted to help somewhat ameliorate the problem of misinformation

The **president of a business** said, "We can use what we already have and perhaps a few more. Libel laws; false advertising laws; laws against breach of contract; laws against making false scientific claims for personal or corporate gain; penalties for victim-targeted hacking and doxxing; laws to protect the integrity of the vote and bar foreign interference in elections; laws preventing corporations from having the rights of people."

Rick Hasen, professor of law and political science, University of California-Irvine, said, "Existing tort law should handle these things. For example, fraudulent conduct leading to damages compensable under current tort system."

A **researcher affiliated with a company and with a major U.S. university** noted, "Manipulation of news should be treated similarly to manipulation of financial data or personal reputation – i.e., subject to legal challenge and legal penalties. Enforcement across

borders will require considerable international work to establish protocols. Interpol, et cetera, and the EU are good starting places."

David Conrad, a chief technology officer, replied, "They should be similar to those for false advertising, perjury, and/or libel depending on context."

A **professor of sociology with expertise in social policy, political economy and public policy** said, "Purveyors must be required to produce clear evidence and, when they cannot, their failures must be publicized."

A **professor at a Washington DC-area university** said, "Government can look to deter some state-based distributors, by, e.g., declaring democratic elections to be critical infrastructure and threatening retaliation for attacks."

An **associate professor and journalist** commented, "The UK has been progressive in tackling trolls through the legal system, so the U.S. could learn from that experience."

Charlie Firestone, executive director, Aspen Institute Communications and Society Program, commented, "We should guard against state censorship, or even corporate censorship that becomes equivalent to state censorship. As for knowingly spreading false info with the intent to create harm, there can be civil actions from those harmed, like libel allows someone to sue for damages."

A **director of new media for a national federation of organizations** said, "They should suffer penalties for treason if this in done in cooperation with a foreign government meant to damage the U.S. political system."

Susan Hares, a pioneer with the NSFNet and longtime internet engineering strategist, now a consultant, said, "In the U.S., slander is treated as a virtual attack on a person. Individuals who plan a destructive riot rather than a peaceful demonstration are criminals. Purposely spreading false information about a company that impacts business can also be considered a crime. Based on these existing legal principles, the government can press for laws that set legal penalties for creating and knowingly spreading bad information. The difficult part of these laws will be the definition of "intent" to create and knowingly spread false information."

A **professor of information studies based in Europe** replied, "Lying and spreading false information with an aim of harming directly or indirectly others should be punishable

as it indirectly tends to be in the current judicial systems. Government and legislators should make sure that winning such cases does not require a lot of wealth, engaging in long-term and unsure cases, and hiring expensive lawyers so that everyone in the society can have an opportunity to win such cases."

Daniel Alpert, managing partner at Westwood Capital, a fellow in economics with The Century Foundation, observed, "Government cybercrime-efforts should track down and confront malefactors and seek to shut them down or block them. But there has to be a transparent judicial process to oversee such efforts."

Helen Holder, distinguished technologist for HP, said, "Penalties should be those for incitement, fraud, harassment, libel, slander, et cetera, rather than any additional or specific penalties. The government could make it easier to pursue these cases. For example, today it is very hard for a person who has been threatened online to take action against their harasser. Often law enforcement is unable or unwilling to investigate. Policy, training, and staffing adjustments could be made to better enforce existing laws and regulations."

A **researcher/statistician consultant at a university** observed, "We need 'ombuds' groups to investigate and apply punitive measures. Punitive measures – loss of employment, if employed. Loss of contract – if on contract. Fines – if unemployed. Also maybe some community work to be completed."

Glenn Edens, CTO for Technology Reserve at Xeroz/PARC, "There should be penalties similar to libel or fraudulent transactions, government should play a role similar to the laws governing consumer protections."

Stowe Boyd, futurist, publisher and editor in chief of Work Futures, said, "What's the legal consequence of yelling 'fire' in a crowded theater? Or libeling or slandering others? We have laws in place that could be repurposed, reinterpreted for our modern times."

Jim Hendler, professor of computing sciences at Rensselaer Polytechnic Institute, commented, "The knowing creation and spread of information that is both provably wrong and done with malicious intent needs to have strong penalties via court of law. Government's role in this would amount to a censorship that would likely be unacceptable – the key phrase is 'intent of causing harmful effects' (illegal might be a better word than harmful) would be what need to be enforced via civic mechanisms and courts."

Leah Lievrouw, professor in the department of information studies at the University of California-Los Angeles, observed, "There are already legal sanctions, even in societies with strong free-speech traditions, on particular classes of information that cause harm: fraud, libel, slander, incitement and so on. These should be revisited and adapted to the online social context. However, I would be very cautious about establishing other, particularistic types of 'harms' that are invoked to restrict speech and information more broadly: blasphemy, disrupting 'public order,' laissez-majesté rules against insulting states or rulers, even some instances of hate speech. The difficulty is balancing individual sensitivities and the wider interest in a diverse, pluralistic, and sometimes disputatious, society."

Sonia Livingstone, professor of social psychology, London School of Economics and Political Science, replied, "I'd treat it like we do the incitement to racial hatred. If there is intent to harm, then the penalty should reflect the intended or actual harm. This must be done by governments not companies, as government is (should be!) accountable to its people."

A **North American research scientist** wrote, "Government is likely the only actor with authority to stem flows of false information. The penalties should be determined by the intent of the harms (and should be very severe for efforts to undermine democratic freedoms and security)."

An anonymous **international internet public policy expert** said, "The government should play a role in supporting prevention and in issuing penalties."

Others said those in government and their support teams are a cause of much of the misinformation. A **head of** systems and researcher working in Web science said, "Government needs to be held accountable as they cooperate with Super PAC agendas that are behind a good number of disinformation campaigns."

A **futurist based in Western Europe** said, "Yes, large penalties should be introduced, the same as for people who give misleading information in financial reports and in advertisements. Of course, this must be overseen by a body that can be understood as being independent, which will be hard. And it will not be a complete solution to the problem of fake information. But it will be an important contribution."

Axel Bruns, professor at the Digital Media Research Centre, Queensland University of Technology, commented, "Possible penalties could range from temporary social media bans to imprisonment, but how these are applied is a matter for the judiciary. The fundamental

principle, however, must be that legal penalties are designed to promote rehabilitation rather than exact revenge; simply locking up trolls and propagandists merely makes martyrs out of them. Government is clearly central here, as it is to all aspects of society: it must get better at *sensibly* regulating traditional, digital, and social media platforms and channels, rather than vainly believing in market self-regulation; it must develop a much better understanding of contemporary media platforms amongst policy-makers, law enforcement, and the judiciary; and most of all it must develop far more proactive means of promoting media literacy in society."

Andrew Dwyer, an expert in cybersecurity and malware at the University of Oxford, commented, "From the perspective of the UK/Europe – we already have systems in place that allow for misinformation to have penalties. Yet these have not been routinely applied online thus far. Developing a body of case law could be a productive way forward. Government roles are and should always be limited."

Tanya Berger-Wolf, professor at the University of Illinois-Chicago, wrote, "We already have most of the penalty system for intentionally harming somebody, including with misinformation (libel, false advertising, identity theft, et cetera). The intention is very hard to prove. However, the punishment, as always, should be commensurate with the resulting harm."

Charles Ess, a professor of media studies at the University of Oslo, wrote, "The penalties should be severe. Rights to freedom of expression have always recognized that speech intended to generate harm is NOT protected speech. As has become manifest over the past two decades, the international corporations controlling most of our communication media have little incentive to regulate or control harmful speech: the more clicks, the better, etc. Democratically elected and responsible governments - i.e., ones that citizens constantly call into account – are the only institutions capable of policing and regulating harmful speech."

Angela Carr, a professor of law based in North America, replied, "I would like to see government step up efforts to enforce the laws against unfair or deceptive marketing practices. Also, I also think more should be done to protect speakers that others try to silence through threats and intimidation. I would like to see Citizens United overturned and effective campaign reform legislation. Beyond these efforts (which certainly seem unlikely in the present environment) I think it is difficult for government to prevent distribution of false information. Not only is it difficult to know whether information is true or false, but it is even more difficult to determine the speaker's intent. Government can, however, encourage the

dissemination of accurate information by supporting public broadcasting, and other non-profit organizations that seek to genuinely inform the public."

Michael J. Oghia, an author, editor and journalist based in Europe, said, "There should be some form of criminal procedure for this, which includes a fine or other appropriate penalty. Depending on the intended effect, prison or internet restrictions could also be options, but governments and law enforcement would have to be involved in this process. I also fear that empowering these two stakeholder groups with such power could be used against, say, minorities and other disadvantaged groups."

An anonymous **internet pioneer and longtime leader in ICANN** said, "Proportionality of response should take into effect all of the costs of the negative externalities created by knowingly spreading the false information."

A **distinguished engineer for one of the world's largest networking technologies companies** commented, "There are outright lies and then there's stretching the truth. Some actions, for example creating widespread panic with fake news, must be prosecuted. There are already civil penalties for slander and libel that extend to the internet. Legislation and definition of this will be a protracted debate. In the immediate future, the penalty will be taking away the source's access and will be done by the content and service providers (albeit a moving target)."

Alan Inouye, director of public policy for the American Library Association, commented, "We already have some well-established laws, such as the rubrics of libel and slander. Perhaps these rubrics need to be revised."

Veronika Valdova, managing partner at Arete-Zoe, noted, "False statements distributed to official authorities as a witness statement qualify as perjury. Adverse information identified during background checks hinders the individual's ability to find gainful employment, get a security clearance, or obtain a visa. If such information turns out to be false, this may be the grounds for a civil suit. Currently, pursuing such suits is difficult because the victim is rarely able to prove the nature and origin of such information and prove a causal relationship between a specific piece of information and rejection. The spread of illegally obtained surveillance material, personal health records, and other sensitive material is illegal under specific laws in most jurisdictions. The right to due process may be the answer. Resolution of such disputes generally belongs to courts. The role of governments is to ensure the resilience of their systems and rigorous assessment of evidence and the prevention of abuse. The

penalties can range from shutting down a single website to no-fly lists for specific individuals."

James LaRue, director of the Office for Intellectual Freedom of the American Library Association, commented, "I suppose libel/defamation laws provide some guidance: a finding of deliberate harm has financial penalties. The government role: rule of law, incorruptible courts. The adequate funding of public libraries to provide sufficient and timely resources to investigate claims."

Sebastian Benthall, junior research scientist, New York University Steinhardt, responded, "Companies should be subject to penalties for deceptive practices as under a strong FTC regime. Defamation should be punished under the relevant laws. And so on. There is ample precedent for the role and limits of government in confronting false information."

Tim Bray, senior principal technologist for Amazon.com, said, "Existing libel and slander laws are adequate. Canada has anti-hate legislation but its effectiveness has really yet to be established."

Adam Holland, a lawyer and project manager at Harvard's Berkman Klein Center for Internet & Society, noted, "I suspect that exisiting law about willfully causing harm, whether physical, emotional, or reputational, will provide a useful template for the actual nature of any penalties. However, intent is extremely difficult to effectively prove, and 'false information' is going to be equally difficult to distinguish from fiction. Penalties, regardless of what they are, will be rare in application. Government should not be taking steps to prevent, since definitions of what is subject to any prevention may well change with the government. Government should empower the citizenry and enforce existing law equally."

Bart Knijnenburg, researcher on decision-making and recommender systems and assistant professor of computer science at Clemson University, said, "Harmful speech should not be protected as free speech. I believe that the European anti-hate speech laws make a lot of sense: if there is an intent to harm others (or move one's followers to harm others), it should be punishable by law."

David Brake, a researcher and journalist, replied, "It depends on the 'harmful effect' sought. If the intent is to incite hatred of others it should be dealt with through hate crime legislation (present already in most countries) or anti-bullying legislation. If 'merely' political then simple ridicule by a free press is the best we can hope for."

Laurel Felt, lecturer at the University of Southern California, "It might be difficult to prove intent. But assuming that one could prove harmful intent, then the government would need to create some sort of policy that condemns such an action. The government body responsible for investigating and prosecuting such cases might be the Federal Communications Commission? Assuming prosecution that culminates in conviction, the penalty could be a fine, I suppose."

Nick Ashton-Hart, a public policy professional based in Europe, commented, "Penalties should be proportional to the ability to harm, and government should step in only to the extent that civil or criminal action to redress harms done are appropriate and proportional."

Jonathan Brewer, consulting engineer for Telco2, commented, "Dangerous speech is not a phenomena unique to the internet. Existing regulations and programs around the world may need to be updated or enhanced, but I don't think any new penalties need be established."

Barry Chudakov, founder and principal, Sertain Research and StreamFuzion Corp., said, "Just as electricity in the U.S. is regulated at the federal, state, and local levels, information is now a force like electricity and needs independent oversight with checks and balances, of course, but with some recourse to signal the deliberate spread of false information and some power to stop it. Penalties for those found to have created or knowingly spread false information with the intent of causing harm should be at least as severe as a class B felony (punishable by up to 20 years in prison, a fine of up to $20,000, or both.) News sources (i.e., CNN, The New York Times, Washington Post, The New Yorker, et cetera) should hold a news reliability summit and devise what might be termed a 'reliability index' … Like the American constitution, there should be a means to amend or improve the reliability index. Once that is in place, each piece of information, or definitive statement, can be assigned a level of certainty or reliability.

"… We have standards of measurement in the food industries and commerce, we have standards of disease and wellness in healthcare, we have standards of tolerance and capacity in civil engineering and aerospace. We can establish standards for information. With a meaningful standard in place, we can establish penalties for violations of the standard(s)… A free press should be able to govern itself without government interference, so the pillars of the press community should establish and jealously guard the integrity of a reliability index. We need to establish clear sanctions and penalties to deter any authority or other entity from designing and spreading *misinformation*, a trendy word for lies. Information is the lifeblood of democratic institutions. Without trustworthy, reliable information … democracy will die."

Bob Frankston, internet pioneer and software innovator, said, "It is dangerous to impose too much control, but maybe there should be a concept of public libel?"

Jane Elizabeth, senior manager American Press Institute, said, "There already are penalties for hateful/dangerous speech and other communications. The penalties for malicious misinformation could work in a similar way."

While legal remedies may work locally at times, the global nature of the internet and variability of the application of law negates their efficacy

Eduardo Villanueva-Mansilla, associate professor, department of communications, Pontificia Universidad Católica del Perú, said, "First, define 'harmful,' then, we will have to deal with the interconnectedness of the systems allowing the spread of such information, and the fact that there are no political mechanisms to punish actions by a citizen from a given nation state in other nation state, even if s/he is identifiable. Sanctions between states are limited and dangerous beyond some very specific scope."

Bill Woodcock, executive director of the Packet Clearing House, wrote, "This is the 'crying fire in an opera house' abuse, generally. The problem is in the transnational nature of the commission of the crime; in the country of origin, it may be a patriotic act, rather than a criminal one. And nations will never curtail their own Westphalian sovereign 'rights' to define what actions are criminal within their borders."

Jerry Michalski, futurist and founder of REX, replied, "I am not a lawyer, but current laws regarding freedom of speech and harmful speech give us a lot to work with. The problem is the anonymity and superconductivity of the Net, along with the global trust implosion. Governments need to address trust more directly."

A **retired professor and research scientist** said, "The government role is hard to accomplish due to the global nature of the internet – e.g., Wikileaks and Julian Assange."

A **chief technology officer** observed, "It depends on the harmful effects. If the actors are outside of U.S. jurisdiction, there is not much that can be done."

Nathaniel Borenstein, chief scientist at Mimecast, commented, "Penalties should be severe, including substantial jail time and fines. But I expect this to be unenforceable across international boundaries."

Thomas Frey, executive director and senior futurist at the DaVinci Institute, replied, "In a world that is transitioning from national systems to global systems, we are desperately in need of a new global watchdog, one that perhaps most nation states are members of, to oversee the creation of policies, rules and enforcement around the globe."

Further legal approaches are not likely to be workable, nor are they likely to be effective

Dan Gillmor, professor at the Cronkite School of Journalism and Communication, Arizona State University, commented, "In a few cases this is already illegal. Expanding laws to punish speech is a step toward a police state. One key government role should be to give schools better incentives to teach critical thinking – specifically media/news literacy – as a core part of the curriculum."

John Anderson, director of Journalism and Media Studies at Brooklyn College, City University of New York, wrote, "We have existing legal mechanisms to combat the spread of false information with the intent to do harm, but our legal system works about two generations behind where communications technology is. Things are not helped by the increased politicization of the judiciary itself."

Jim Warren, an internet pioneer and open-government/open-records/open-meetings advocate, said, "Accuracy of information is NOT binary. It is a continuum. Additionally, proving intent makes legal or governmental penalties VERY difficult; even moreso when government agents, themselves, are the perpetrator. If there is substantive harm from such disinformation, defined by law, then those same laws need to include penalties and enforcement procedures. We have ample precedent for this (difficult!) situation, in the form of slander and libel laws."

Stephen Downes, researcher with the National Research Council of Canada, commented, "Using existing laws, we can assess penalties based on actual damages caused, in those few cases where actual prosecution is possible. But given that government and large corporations profit the most from spreading false information, it seems unlikely they can be trusted to take any steps to prevent it. There is probably no legal remedy, because the people who benefit from misinformation have been the ones to write the laws."

A **vice president for a company based in North America** replied, "Left to its own devices, the market will likely begin reputation tracking (similar to the reputation tracking of eBay). Bad actors would suffer loss of reputation and influence. Let the market of ideas work

out its own solution. Keep government meddling to a minimum; it's almost universally destructive."

Free speech is a pivot point: Regulatory mechanisms may stifle unpopular-but-important speech just as much or more than they stifle harmful speech

Kenneth Sherrill, professor emeritus of political science, Hunter College, City University of New York, said, "I'm a hard-core, empirical, quantitative scholar. We think that good information drives out bad information and that systematic liars are shunned. This is wishful thinking. I don't want the government to decide what information is false… The only answer is to be found in free speech and the marketplace of ideas. This is why I'm so pessimistic."

Paul M.A. Baker, senior director of research for the Center for Advanced Communications Policy, said, "The consequences and penalties of knowingly spreading false information is a tricky balance. In a private setting, operation of market mechanisms/self-regulation would seem to viable approach; in a public setting the balance between free speech and protection of vulnerable populations must be maintained. For willful promotion/distribution of dangerous or harmful material it would seem that the judicial process is appropriate. Use of regulatory mechanisms while possible run the risk of stifling both dangerous, as well as unpopular speech. The latter could be a case of criticism of an administration which might be valid."

Adam Powell, project manager, Internet of Things Emergency Response Initiative, University of Southern California Annenberg Center, said, "No, and therefore none. Remember, 'Congress shall make no law….'"

Garland McCoy, president, Technology Education Institute, commented, "Who defines 'false information'? Many argued at the time that Orson Welles should have been put in prison for his ground breaking radio broadcast of 'War of the Worlds.' So the government or mob rule should hang a modern-day Orson Welles?"

A **professor of law at a state university** replied, "I have no problem with criminalizing knowing false statements. That is not in my view free expression. But the Supreme Court has often protected lying in politics. We need a constitutional amendment – but of course will never get it."

A **principal research scientist at a major U.S. university** replied, "One person's harm is another person's virtue. The government can't impose penalties without running afoul of the First Amendment."

Rick Forno, senior lecturer in computer science and electrical engineering at the University of Maryland-Baltimore County, said, "This is a hard issue to enforce, since in the U.S., First Amendment protections prevent prosecution of even the most moronic 'fake news' items."

Carl Ellison, an early internet developer and security consultant for Microsoft, now retired, commented, "Seventy years ago, such a source would be denied air time. We no longer have limited channels. We can apply economic sanctions against Russia but what power do/should we have against Breitbart or The National Enquirer?"

Geoff Scott, CEO of Hackerati, commented, "Knowingly spreading false information is a form of taking away people's right of self-determination and it is an extremely heinous act that should be severely punished. On the other hand, what constitutes 'false information'? The First Amendment exists for a reason; but some forms of speech are not protected, and these have been clearly defined. How would 'False Information' be defined in the context of the First Amendment?"

Steve McDowell, professor of communication and information at Florida State University, replied, "It will be easier for private-sector actors to proceed as they already do, and make commercial decisions about their policies. Civil law remedies for defamation, libel, and privacy protection already are in place, and if other types of harm can be identified, there may be civil law approaches that can be followed. Since many stories may originate outside the country, this approach may have significant limitations. It will be more difficult for the government in the United States to be involved in such efforts, given the strong First Amendment traditions limiting government actions concerning speech and expression."

Matt Armstrong, an independent research fellow working with King's College, formerly executive director of the U.S. Advisory Commission on Public Diplomacy, replied, "Our modern view of the First Amendment is perhaps 100 years old. The malicious creation and spreading of information is an intent that can be pursued, however this will not be successful tactic unless society and government are unified behind this approach. At present, the creation and spread of intentionally false and harmful information plays into a divisiveness that must be addressed first. It is very close to a chicken and egg conundrum, but we have to start somewhere."

The misinformation conundrum
presents too many complexities to be solvable

Matt Moore, a business leader, commented, "I am not sure that there is a public appetite to enforce penalties for doing this. We need people to take public responsibility for both what they say and what they consume. This needs to come from the top. And it is manifestly not happening."

Noah Grand, a sociology Ph.D., wrote, "I understand why there is a lot of anger toward people who knowingly spread false information. Punishing these deceivers seems very appealing. Unfortunately, punishment won't do anything about the people who want to be deceived. America's 'War on Drugs' – with its emphasis on punishing suppliers – hasn't been very effective. There's always a new supplier who rushes in to fill the demand. Why would we expect something different from a 'War on False Information' that targets suppliers?"

An anonymous **CEO and consultant based in North America** noted, "Trying various enforcement models on the current internet is just a waste of time. They won't solve the overall problem."

An **internet pioneer/originator** said, "Defamation of Public Trust depends on who defines 'The Public' doesn't it? And that is the fundamental problem that will always remain."

An **analyst at Stanford University** commented, "I can't imagine who would adjudicate this. What is 'harmful effect?'"

Stephan Adelson, an entrepreneur and business leader, said, "The enforcement of this type of oversight sounds like an impossible task. Ideally repercussions for spreading harmful untruths should exist but the expense of monitoring and pursuing those guilty would be immense. I can't imagine the government being put in the position of determining what truth is determining what harm is and then pursuing those they have determined to be spreading harmful untruths under their own definitions."

Jack Schofield, longtime technology editor at The Guardian, now a columnist for The Guardian and ZDNet, commented, "You can't fine or lock people up for spreading false information, because there's too much information to fact-check, and because it's sometimes quite hard to separate fact from opinion."

A **leading researcher studying the spread of misinformation** observed, "We don't currently don't have the ability to know which actors spread false or harmful information, or even who pays for this type of influence. There are few rules in digital political advertising in the United States, for instance. While campaign spends are recorded with the Federal Election Commission, there is no record or detailed log of what was promoted/placed, who was exposed to messages, or how these messages (ads, sponsored posts, 'dark posts,' et cetera) were executed on and delivered through data mining. This isn't like a campaign mailer or newspaper ad for a political candidate that we can clip out. Since there is no way to trace large-scale political influence operations back to specific actors, agencies

Howard Rheingold, pioneer researcher of virtual communities, longtime professor and author of "Net Smart: How to Thrive Online," said, "Criminal penalties might infringe on free-speech rights, but identifying known liars and purveyors of false information and providing links to proofs that their information is false - enabling reputation to enter the equation - could be helpful. But then the smartest purveyors of false information will shift identities."

Jason Hong, associate professor, School of Computer Science, Carnegie Mellon University, said, "Applying penalties to people who spread false information is a good idea in theory but incredibly hard to do in practice. For domestic cases, how can we differentiate from stupidly but innocently jumping to conclusions vs. deliberate misinformation? How to differentiate between legitimate grassroots campaigns vs. organized groups deliberately aiming to spread misinformation? How to identify domestic groups or individuals vs. foreign ones that local governments have little leverage over? There aren't many good options here, especially when the bulk of misinformation today is substantially benefiting one of the two main political parties in the United States. What the government can do is to hold hearings to do basic fact finding, and offer research funding/competitions to disincentivize and/or block the most widely agreed upon and egregious cases."

A **former software systems architect** replied, "Civil/criminal penalties that exist can continue. The problem is identifying the culprit, demonstrating that is knowingly false (or not verifiably true), and it being harmful. The problem is identifying harmed parties."

An anonymous **professor of information science at a large U.S. state university** wrote, "How do you judge whether it is false information or not? It may simply be one's opinion, or it may be created and spread for national security purposes. Some false information doesn't really cause too much problem for other people and the society."

Adam Gismondi, a researcher at the Institute for Democracy & Higher Education, Tufts University, observed, "It is hard to overstate how delicate the approach must be on these questions. If this problem isn't approached in a way that transcends partisan politics, it will forever be dragged down by polarized perspectives. Until there is a collective recognition of facts around false information and the harm that it causes, the idea of penalties and a role for government in the matter is a non-starter."

Philip Rhoades, retired IT consultant and biomedical researcher with Neural Archives Foundation, said, "Separate, non-falsifiable networks need to be established as alternatives. It is not going to be possible contain the powerful 'bad actors' who basically own the system."

Larry Keeley, founder of innovation consultancy Doblin, observed, "We should spank them and send them to bed without any supper. ;-) The solution to bad information is always better information."

An **anonymous respondent who works with the Berkman Klein Center at Harvard University** noted, "People who knowingly spread false information can suffer civil penalties… But how do you measure or quantify the damage done by spreading false information? Is it enough to decide that it causes measureable harm to individuals? How can we quantify the effect on our civil systems of governance and information sharing, on the integrity of the social contract that all members of a community act without intent to harm or deceive their fellows?"

Philipp Müller, postdoctoral researcher at the University of Mainz, Germany, replied, "It is impossible to judge whether the intended effects of spreading a certain information are 'harmful.' Therefore, I see no way how this could be punished. If false information harms existing laws (e.g., against insult or demagoguery) the source should be punished according to these existing laws. If false information is spread with the intention of, e.g., political campaigning without harming any existing law, we cannot begin to punish this. This would undermine freedom of expression. The consequences of this would be harmful to a much greater extent than any misinformation could be."

A selection of additional comments by anonymous respondents:
- "Manipulating society is a crime."
- "Freedom of speech means there is no crime in this."
- "Before taking any steps, we need to define what 'false' and 'harmful' means."
- "The key is to reduce incentives at the elite level for spreading misinformation."
- "Those spreading false information should be cut off from systems they use to do it."

- "Sanctions should be available to prevent spreading of fake news inciting violence."
- "The government should not be the arbiter of truthfulness."
- "I don't really think government should censor information even if it is false. I'm with Milton in that way."
- "I do not believe most people who create fake news believe that they are working for a cause that will have harmful effects."
- "It would be impossible in today's environment to get consensus on what counts as 'false information.'"
- "The burden of proof required to make this case is too high to make penalties effective."
- "Government is very often the problem. We should let the people decide, not some political ministry of truth."
- "Read Plato's 'Gorgias.' Hold the gullible accountable for culpability."
- "There could be 'reputation penalties' for such actors. Similar to how platforms like Reddit keep their bad apple in check, there could be a universal reputation bank for all internet users."
- "Those spreading the information are unlikely to be in the targeted jurisdiction, and are likely to be operating with the tacit or explicit support of their jurisdiction."
- "It will be hard to police the spread of false information because truth is a nebulous concept. Creating trusted, reliable sources for information is a better strategy than punishing liars."
- "Focus on creating a robust civic infrastructure. Government plays a big role in that."
- "Individuals should be fined or sanctioned. Government might establish expedited courts to enforce this."
- "The intention to cause harm is in this case the legally actionable quality. We have laws against hate speech for example, which might be extended to hatred aimed at non-humans, which might include climate change denial if the intention is to harm the environment."
- "We need better data around who has been truthful."

Follow-up #5:
What do you think will happen to trust in information online by 2027?

The answers to this question were widely spread. A **professor** based in North America wrote, "The level of trust will be very low." A **policy analyst for the U.S. Department of Defense** wrote, "Trust will improve." A **senior research scholar at a top-ranked U.S. law school** wrote, "Trust will remain high within filter bubbles of information, trust in adversaries' bubbles may climb some." A **professor and research scientist based in Europe** commented, "Nothing will change. The balance between trust and distrust in information will be approximately the same." The reasoning behind these opinions varied.

Susan Etlinger, industry analyst, Altimeter Research, said, "Technology has created an information arms race that is very similar to what we see with cybercrime and hackers. My guess would be that information ecosystems will behave similarly: periods of relative apathy punctuated by panic and outrage."

Virginia Paque, lecturer and researcher of internet governance, DiploFoundation, wrote, "We are entering into a period of open and serious skepticism of any information, online or offline. I hope that this will quickly be followed by implementation of tools to address this both on and offline, and we will have recovered before 2027. The internet will require a quick response time [to this issue] to maintain its usefulness."

Amy Webb, author and founder of the Future Today Institute, wrote, "We've become conditioned to share before we read all the way through a story, or before our common sense kicks in. We're also slaves to our amygdalas, and this moment in human history is rife with economic uncertainty, geopolitical anxiety and wild stories about the future of transformative technologies like artificial intelligence and genomic editing. Given what we know to be true today, it's clear that we're on a dangerous path towards the future. Without significant changes, the public trust of quality news will continue to erode, which inevitably contributes to the financial demise of our once-lauded news organizations. Without trained investigative reporters, copy desks, producers and editors, we'll find ourselves drowning in information but without any sense of which paddle or tree branch to grasp onto for help. Around 2027, people and the artificially intelligent systems that work alongside and augment them, could have to make decisions based on a cesspool of misinformation, misleading statistics, rumour, innuendo and whatever's left of our trusted news organizations. It's a bleak outlook, but here's something important to keep in mind: that future hasn't happened yet. The future has

always been our shared responsibility in the present. When you stop to think of the critical role that you, personally, play in what's over the horizon, it can be very empowering. And, by the way, that's a good way to keep your amygdala in check."

Scrutinizing the very notion of trust…
And, what is "fact," what is "truth"?

The reasoning behind opinions on this question were wide-ranging. Some people discussed the very notions of trust and truth.

A **professor of education policy** commented, "This process of thinking about how you come to 'trust' is very different than 'trusting' information Channel X. The notion of trust is so multifaceted. Trust that some information is 'true,' for example, is very different than trust that a particular source 'speaks' your language. The danger that psychology and economics researchers have shown us is that people like to hear what confirms preexisting biases. So, a form of trust can easily grow from confirmatory sources, but this is not a form of trust we would want to nurture as a country. What is often missing from this discussion so far is not technological fixes, but educational/behavioral fixes. We need to unplug, we need to listen to each other, we need to be cautious about trusting because we are able to weigh evidence and seek out multiple sources that we can weigh against each other."

A **research scientist based in North America** said the concept of trust is morphing, commenting, "With all the forms of manipulation possible with digital information, the boundary of fake and true will blur, trust will transform with it."

John Wilbanks, chief commons officer, Sage Bionetworks, replied, "Trust is a word that gets redefined by new generations with new access to information. So this isn't about 'trust' but about 'what we thought trust was before it got subsumed in an information flood.'"

Ian O'Byrne, assistant professor at the College of Charleston, replied, "Some bad actors will be prosecuted to make us believe something has happened to address these issues. [But] business, governments, and organizations will continue to spread these digital texts and tools and play it 'fast and loose' with our rights and liberties. Our online tribes and affinity spaces will continue to fracture and solidify as we find more in common with the collection of friends we have online than we do with the people on our street, state or country. Trust and truth will be different commodities for different individuals in and across these spaces. Everyone will have trust and truth. It will just mean different things for different people."

An **anonymous respondent** wrote, "Trust isn't often related to actual presence of factual content, at least not much. Trust in information will continue to decline and – paradoxically – this decline will occur despite the fact we have gotten better at stopping it."

danah boyd, principal researcher, Microsoft Research and founder, Data & Society, wrote, "We are going to see more and more adversarial attempts to gaslight the public. This is not specifically about the internet. This is about who trusts what."

Ian Peter, an internet pioneer, historian, activist user and futurist, replied, "Trust *should* deteriorate, and we all should become far more critical of what we read and are told, but I am not sure whether that will eventuate. We are more likely to carry on trusting information as if nothing had happened and just believe whatever we are told we should believe."

David Manz, a cybersecurity scientist, replied, "Trust is an attribute of a relationship between two human beings. You don't trust a chair to hold you. You trust the maker, the installer, the last user, etc. Similarly in the use of computers we might anthropomorphize them but at the end of the day it is trust between the human content creator, the distributor, the echo chamber, your peers and finally you the consumer."

Garth Graham, an advocate for community-owned broadband with Telecommunities Canada, explained, "We will begin to realize that truth/lie is a false dichotomy, and that 'information' is a verb, not a noun. Also that narrative is an illusion. We are discovering that mind/consciousness depends on context. The internet increases our awareness that reality is a construct. It accelerates our capacity to apply that awareness. If we are lucky, by 2027, we will be able to practice that capacity as a learned artifice. We will be more conscious of the nature of consciousness. As we do this, our trust in 'society' as an organizing principle dependent on external authority will disappear. To be replaced by a reliance on self-organizing community as the primary principle of structural relationship and organization."

Sean Justice, assistant professor at Texas State University-San Marcos, "This is an ecosystem question if 'trust' is held as an open, relational term. In that sense, 'trust' will continue to be commodified in capitalist systems. But another question needs to be asked simultaneously, how is capitalism changing? Changes to the materiality of the ecology have yet to be theorized in a coherent way. Questions that rely on anachronistic (black-boxed) terminology might actually work against a sustainable dialog that might prove useful, however. In the end it might not matter too much that we understand what we're doing; practice often (perhaps always) leads theory."

The rise of misinformation will continue, and things will likely worsen

Many respondents argued that action must be taken or there will be dire results and others expressed worry, disappointment, sadness or resignation.

Jerry Michalski, futurist and founder of REX, replied, "I'm afraid we won't make much progress in a decade. It's too early. The possibilities for havoc haven't yet been played out, believe it or not."

Andrew Nachison, author, futurist and founder of WeMedia, said, "We're losing trust in everything, including the institutions we need to sustain a civic, civil, peaceful liberal society. We need to rebuild trust in everything. Short of that, by 2027 we will be stuck in a century of endless wars, terror, corruption and injustice. Who will lead us to a better future? That's the real question we and our children will face."

Tom Rosenstiel, author, director of the American Press Institute, senior non-resident fellow at the Brookings Institution, commented, "The last 30 years suggest that the forces of declining trust will likely continue. Three trends are merging here. As technology expands, the audience fragments further into its own channels by subject and point of view. And as that happens, political leaders, particularly those who feel the traditional media are against them will continue to exploit of that to inflame audiences for their own purposes."

Dean Willis, consultant for Softarmor Systems, commented, "By 2027, online information will be as trusted as (the Russian news service) Pravda."

An adjunct **senior lecturer in computing** said, "In 2027 people won't even trust information from many of their family and friends, let alone online information that disagrees with their own view of the world."

A **professor of media and communication based in Europe** said, "If no substantial measures are taken to avoid and prevent the pollution of the internet, online information by 2027 will be regarded as sewage."

Tiziano Bonini, lecturer in media studies at the department of social, political and cognitive sciences, University of Siena, said, "Information online will be extremely polarized. Most of the information will be under the real-time review of millions of skilled users, while bad actors will continue to proliferate in subcultural contexts or specific clusters of people

(those less skilled in media literacy). Authoritarian governments will centralize and control information online, producing fake news themselves. Trust will more and more rely on single persons (journalists and gatekeepers with a high reputation, maybe measured through new ranking systems) instead of single institutions."

A number of people mentioned that emerging advances in technology – including manipulation of audio, video and VR and AR information – today make it clear that by 2027 it is highly likely to be even more difficult to understand if information is fake or real.

David Conrad, a chief technology officer, replied, "It will continue to decline, particularly as technology evolves for modifying and/or generating fake video, audio and text that is essentially indistinguishable from real information."

Judith Donath, fellow at Harvard's Berkman Klein Center, and founder of the Sociable Media Group at the MIT Media Lab, commented, "There will be an arms race of fakeness, especially in audio and video, as the tools to make convincing artificial videos of people and events become commonplace and believable."

A **postdoctoral associate at MIT** said, "In the next decade we will see the rise of false (but completely realistic looking) audio and video segments on the internet. Textual misinformation (such as fake news) will be the least of our worries by then."

A **software engineer based in Europe** said, "Given recent experimentation with spoofed speech and videos, people are only going to have to pay much more attention."

A **professor at Harvard Business School** said, "2027 will be much the same as today, but with even-more-sophisticated videos and other fakes."

The **managing partner of a technology consultancy** wrote, "The notion of empirical facts based on physical law, observation, research and/or corroboration may be jeopardized as we merge the physical world with virtual world (fueled by pervasive AR/VR/mixed reality) and 'facts' can be created with the attributes of authenticity, corroboration and evidence yet false or harmful."

A **business leader based in Europe** wrote, "We'll see more and more deception, not only fake news as they are now – but also more elaborate schemes – like placing fake information proactively in files that are in danger to be leaked."

A **planning information manager for an East Coast city** said, "Trust will deteriorate significantly, with people breaking into even-more-moated constituencies for obtaining information."

A **professor of rhetoric and communication** said, "People will be even more isolated in their silos, reticent to accept any information that does not cohere with their existing beliefs."

A **graduate researcher based in North America** commented, "People will only trust the small range of sources that align with their viewpoints and general trust will decrease dramatically unless we can curtail the spread of false news."

A **futurist/consultant** said, "If we don't engineer greater trust we may see a more balkanized/tribalized society, which could become ungovernable on the scales we are familiar with."

Alan D. Mutter, media consultant and faculty at graduate school of journalism, University of California-Berkeley, replied, "I am terrified to contemplate the subject… Even as I cling to the hope that the arc of history will right itself, I doubt anyone will ever again be regarded, Walter Cronkite-like, as 'the most trusted' person in America."

Mercy Mutemi, legislative advisor for the Kenya Private Sector Alliance, wrote, "Trust will disintegrate."

Adam Holland, a lawyer and project manager at Harvard's Berkman Klein Center for Internet & Society, said, "It will in general decrease, as the sheer amount of what is available proliferates. Alongside this trend, information consumers will also *increase* trust in information from *certain* people or outlets. This trust will sometimes be warranted, but it will also be the result of avoiding cognitive dissonance or (virtue), signaling tribal allegiance."

Fredric Litto, professor emeritus, University of São Paulo, Brazil, wrote, "It will be increasingly diminished, much as we currently witness, dividing every community into 'tribes' organized by ideological, economic, religious and other cultural criteria, thereby augmenting extreme stress in everyday life, with unpredictable, long-range, consequences."

An **internet pioneer and principal architect in computing science** replied, "Overall trust in all online activity will decline markedly over time, due to mass compromise of information systems. This will lead to legislation, holding firms liable for negligent security practices. After that, trust will improve."

A **media networking consultant** said, "Online information will be more resilient to hacking but there will continue to be a growing number of sources of information and not all will be reliable."

A **principal technology architect and author** replied, "It will decrease – but there will be so few sources that it will not matter. The entire ecosystem will fall under the control of a few players, and 'we will believe what we are told to believe,' unless we have some alternate form of information, which will only be local. Hence we will end up in a situation where every piece of local knowledge goes against the larger picture we are being told to believe, but everyone will believe the larger picture because 'it must be different everywhere else.'"

A **technical writer** said, "Trust in information will be nonexistent."

The **dean of one of the top 10 journalism and communications schools in the U.S.** replied, "There is financial and political gain from false information, so it will not cease. The focus should be on how to counter it in new forms."

An **anonymous respondent** replied, "All information will require repeated authentication by individuals and organisations and even then we can take it with a pinch of salt, or we can simply live in the hope that false information will stop :)."

An **author, editor and journalist based in North America** replied, "Not much good will happen in the next decade. We're pretty doomed."

A **professor at a major U.S. university** replied, "Trust will decline, creating incentives for a balkanized internet, with different parts of it offering differing degrees of encryption and consumer protection."

Daniel Berleant, author of the book "The Human Race to the Future," commented, "Trust will decline, as society becomes more polarized and more segmented into parochial special interests. If and when society turns a corner and prevailing values begin to favor the common good, trust may begin to increase, but there is no particular reason to believe this will occur soon."

Bernie Hogan, senior research fellow, University of Oxford, said, "I'm sure we want to believe it will get better, but I assume that instead it will get more effectively manipulated. Those on the right are increasingly suspicious of institutions and those on the left are suspicious of many actors that do not pander to their specific cause. Personalised,

demographically appropriate celebrities will be increasingly available to appeal to specific groups. A cataclysmic event such as a pandemic or world war might disrupt this trend, wherein we reevaluate the overall state of information distribution. Barring that, I imagine it will be business as usual, with people trusting what they believe in, in the most convenient, smallest doses possible. I mean we would much rather buy an intelligent agent that tells us what we want to hear than one that tells us what we should here to engage in politics beyond the local level."

Kelly Garrett, associate professor in the School of Communication at Ohio State University, said, "In 10 years' time individuals and societies will have developed new strategies to keep online deception in check, and Americans will have found renewed faith in some type of authority… Unfortunately, some bad behaviors will have been normalized, and new threats to our ability to know what to believe will emerge. Ideological divisions will remain sharp, and beliefs will continue to fall along party lines. Foreign powers' attempts at political manipulation via disinformation will be more commonplace. And technologies for fabricating audio and video recordings of events that never happened will be widely known, and regularly abused."

Glenn Edens, CTO for Technology Reserve at Xeroz/PARC, "Truth now seems 'optional.' The root of these issues is in publishing and consumption as well as education. We may get to a point where 'media' is largely ignored, especially in an environment where the boundaries between business and editorial barely exist anymore. With any luck, society will self-regulate and it will be cool again to verify sources and fact-check."

Bill Woodcock, executive director of the Packet Clearing House, wrote, "I'm afraid the trolls will continue to ascend over the next decade, with national sponsors and a growing sense that it can be hip to be reactionary if you can play the left for rubes. Which leaves the schoolchildren of tomorrow unable to trust either textbooks or the internet."

The next few years are crucial to the future of the information environment

Some respondents expressed uncertainty about what will happen to trust in the next decade or said the likely future will be determined by actions and events in the next few years.

David Sarokin of Sarokin Consulting, author of "Missed Information," said, "Continued deterioration will set back science, journalism and liberty, but hopefully, we're smarter than that."

Evan Selinger, professor of philosophy, Rochester Institute of Technology, wrote, "How much trust is given to online information in 2027 will be determined, to a large extent, by whether society comes to its senses and recognizes: 1) That democracy requires quality investigative journalism; and, 2) That this, in turn, requires financially supporting the organizations and companies that can provide it. Algorithmic policing of content and generation of content shouldn't be fetishized as forms of solutionism."

Pamela Rutledge, director of the Media Psychology Research Center, said, "Trust in information depends on individuals taking action and responsibility on their own behalf. If we try to offload responsibility, we will give away freedom."

A leading **researcher studying the spread of misinformation** wrote, "What happens in 2027 will completely depend on what happens in the next five years. Legislators on both sides of the U.S. political spectrum will need to get tough on regulating funding sources, outside influence, and work to increase transparency in marketing and advertising. There will also need to be a joint effort between technology companies, international organizations and public-advocacy organizations to find working solutions for some of the problems that have disrupted civil discourse and more moderate/centrist social and political viewpoints. If this doesn't happen soon, it's unlikely to get better in 2027."

Giovanni Luca Ciampaglia, a research scientist at the Network Science Institute, Indiana University, wrote, "Different sectors of society will have to work together; this includes the press and the social media companies whose platforms connect society with information. And we will need to improve our understanding of these digital information networks to make this happen."

A **publisher** said, "By 2027, either we will have devolved into a splintered isolated society or we will have collectively moved beyond the problem out of necessity."

An **international internet policy expert** said, "Trust in 2027 will ultimately depend on the strength of the democratic governance models that exist. If these models remain then there will be trust."

Susan Hares, a pioneer with the NSFNet and longtime internet engineering strategist, now a consultant, said, "Two futures exist for the internet. One option is that internet service providers decide that they will no longer offer the 'free unfiltered service' and provide only clean data. This level of service will clean out many bots, attacks and pornography. In the second, the internet service providers will continue to have two services: trusted and

'anything goes' internet. Businesses and individuals will desire information that is trusted – so a portion of the internet will have the 'high-trust' information."

Paul Gardner-Stephen, senior lecturer, College of Science & Engineering, Flinders University, said, "Fake news is simply too easy to create, the general population too easy to influence, and the potential benefits of its application too great for power-hungry entities to ignore. It is only if we find ways to defuse these factors, that we will see a long-term improvement in the situation… This is an arms race, just as with spam, malware and other digital blights. Battles will be won and lost, and although the war currently shows no end of ending, the increasing awareness of manipulation will likely mitigate the overall impact of fake news over time."

A **senior principal and author** wrote, "It depends on what interventions are made to encourage the public to separate fact from fiction. Right now, people trust whatever reinforces their worldview."

O'Brien Uzoechi, a business development professional based in Africa, replied, "If misinformation continues to go on unchecked, trust will become a trash word in 2027. But, with appropriate laws and the right application of development through technological commitments there could be a turnaround in our trust in information dissemination by 2027."

Alejandro Pisanty, a professor at UNAM, the National University of Mexico, and longtime internet policy leader, wrote, "The landscape of trust in information online by 2027 will continue to be mixed. There are reasons to project into the future that alkaline diets, science denial, conspiranoic theories, hate and ignorance will not be abated in 10 years. On the other hand, a better understanding of biases and a decade more of the internet's life may begin to create information resources whose trustworthiness is better established and more easily identified, as has taken the press more than 500 years to, somewhat, achieve."

An **associate professor at a major Canadian university** wrote, "We may be at a turning point now, in which the pushback against misinformation will result in a reduction, in which case the trust level will likely stay the same. However, if this issue is not tackled effectively, we will see a reduction in trust of online information and a partial return to more traditional notions of authority, based on known publishers and authors."

Michael R. Nelson, public policy executive with Cloudflare, replied, "New business models and new techniques that harness AI, digital watermarking and more powerful forms of

crowdsourcing will mean more information is verified and reliable. But there will also continue to be deep oceans of misinformation, doctored images and even computer-generated video that portray things that never happened in very convincing and realistic ways."

A **professor of law at a major California university** said, "I would like to think we will have become very good by 2027 at discerning what is false or misleading and what is not. However, humans have always been taken in by frauds, scams and misinformation. Fundamentally, it seems unlikely that we will get much better at discernment on an individual level. Online services may become better at sifting some information out. We may have to come up with a way to better scale our legal system's protections against false information."

Greg Wood, director of communications planning and operations for the Internet Society, replied, "I am hopeful that systems and practices will be developed and deployed that improve the ability of internet users to better verify online information and its sources. However, it is not clear if the economic and other drivers to do this exist. And, practical incentives to spread false information will remain."

A **professor and researcher of American public affairs at a major university** replied, "There will always be information sources at the extremes; the question is whether they continue to have influence."

Mike Roberts, pioneer leader of ICANN and Internet Hall of Fame member, replied, "Trust in information will generally be higher, but perhaps not viewed as high enough."

Barry Chudakov, founder and principal, Sertain Research and StreamFuzion Corp., "Trust in information online will erode if media outlets do not position themselves and their media vehicles to build trust-measures into their content. Just by generating information we will not, magically, generate tools to better regulate that content – any more than driving your car down a road would magically generate road signs and traffic signals along that road. Keeping in mind the need for open access, transparency, and protection of privacy, online information sources will have to cooperatively generate new 'rules of the road' for online information. User-generated content will continue to explode in the next decade. Virginia Tech's 'Evaluating internet information uses five criteria to determine the trustworthiness of online information:

1. *Authority* (Who is this person? How is he or she qualified?)

2. *Coverage* (How relevant is this information? Does it fully address the significant issues associated with the topic?)

3. *Objectivity* (Does the information show minimum bias? Are there links or ads that show the author's agenda?)

4. *Accuracy* (Is the information reliable and error-free? Is there some kind of fact-checking confirmation of the information?)

5. *Currency* (How recent is the information? When was the page last updated?)

"Readers need guidance, filters, standards. The information flood is here, and with it come truly positive outcomes and opportunities. But it also brings consequences, foremost of which is the need to manage that information – give the reader perspective and tools to coordinate the information with other information and ultimately evaluate its worthiness. For example, users can upload social media posts, links, images, or other content to Check, an open web–based verification tool developed by Meedan, as part of their verification process: 'Once an item is uploaded, it can be color-coded and tagged by subject matter. Users can regularly update the status of their reporting, add notes, and include other details that might be useful.' (Neiman Lab: http://bit.ly/2tDB2yi]

"By 2027, hackers and mischief-makers will use technology advances to create more confusion and work to obfuscate or distort the truth. Now is the time to build vigilance and standards into our information. Magical thinking or wishing this to get better is foolish. We must get to work now or by 2027 the nonsense one hears today – you can't trust any information anymore – may, like Orwell's 'doublespeak,' distort reality enough that people will assume it is true.

"As William D. Lutz has written:'All who use language should be concerned whether statements and facts agree, whether language is, in Orwell's words, 'largely the defense of the indefensible' and whether language 'is designed to make lies sound truthful and murder respectable, and to give an appearance of solidity to pure wind.' By 2027 online information can puncture illusions, but only with vigorous attention to building confirmation tools that underline facts and foster truth-telling."

Some people will be smarter about finding and relying upon trusted sources

A share of respondents expressed the hope that people will evolve new ways of dealing with the increasing volume of information of all types in ways that serve the best interests of the common good.

Sonia Livingstone, professor of social psychology, London School of Economics and Political Science, replied, "I really hope that the public will become much more discerning, sceptical and mindful of information quality, source and intent. Will it? Yes, for the mindful – the educated, the politicised, the angry, probably not for everyone else. I can't foretell which will be in the majority – that depends on some other things like the economy, geopolitics, etc."

Esther Dyson, a former journalist and founding chair at ICANN, now a technology entrepreneur, nonprofit founder and philanthropist, expert, said, "I'm optimistic because I'm an optimist. However, there is not a lot of evidence [to support that] right now."

Bob Frankston, internet pioneer and software innovator, said, "Ideally there will be a more-aware public less apt to accept 'the internet says'? Or will there be more acceptance of one's tribe as authority?"

A **member of the Internet Architecture Board** said, "More people will be more sophisticated in how they consume information; they will be less likely to trust it blindly (and that's a good thing). Some people will remain relatively unsophisticated, and thus open to manipulation. The proportion between sophisticated and not will matter, a lot."

Matt Mathis, a research scientist who works at Google, said, "We will get smarter at separating facts from alternate facts."

Jonathan Grudin, principal design researcher, Microsoft, said, "People will develop a more sophisticated awareness of where to find trustworthy information by 2027. This may have taken a century for print media; we can get there faster."

Jamais Cascio, distinguished fellow at the Institute for the Future, said, "There are multiple scenarios. We could be so mistrustful of online information that we look for alternative media of communication for trustworthy material, each potentially worse than the last; we could successfully develop tools and norms to push back against falsehoods (e.g., reliance on general public camera swarms as verification of video). We could be so polarized that people will trust information that comes from ideologically aligned sources and everything else is garbage. I suspect trust in information will be greater by 2027, largely because it will be easier to block out information and information sources that we don't like."

Tim Bray, senior principal technologist for Amazon.com, wrote, "I believe that the people pushing the lying stories also have an explicit political agenda, and once that agenda is discredited, the effect on lying-as-a-strategy will be salutary."

An **internet pioneer who has worked with the FCC, ITU, GE and other major technology companies** commented, "People will rely on trusted sources. The rest will be suspect."

Charlie Firestone, executive director, Aspen Institute Communications and Society Program, commented, "People will be skeptical of information online, but most (or at least many) will have the skills to determine the truthful sources if they care to."

Iain MacLaren, director of the Centre for Excellence in Learning & Teaching, National University of Ireland-Galway, commented, "The default position, which is taking shape even now, will be that of not taking seriously information that is not backed up by evidence or which is part of an obvious 'high shock' deluge. Just as we have developed the ability to screen out many of the ads that plaster websites, so too will we see much of this type of 'information' as electronic noise."

A **researcher based in North America** replied, "We are still living in the wild west of online information. No doubt, entities will be increasingly sophisticated in their ability to create 'realistic' fake information. But at the same time, people will be more aware of the phenomenon and will seek reliable markers for credibility. Technology tools will support this. But also traditional methods, such as information/digital literacy instruction."

Geoff Scott, CEO of Hackerati, commented, "I hope parents and educators will begin teaching their children the critical thinking and investigative skills needed to render fake information harmless, but it will take several more decades before enough people think independently enough to have an impact."

A **consultant based in North America** said, "Trust will decline overall. But there will be sources that enjoy high degrees of trust among particular audiences. Trust in media, like its production, will likely continue to decentralize."

A **professor of information systems at a major technological university in Germany** commented, "We will gradually get up again by 2027, after falling heavily between 2017 and 2022."

Amber Case, research fellow at Harvard Berkman Klein Center for Internet & Society, replied, "Right now we're in a serious emotional time with information. It can trigger intense feelings and reactions that make it difficult to make sober choices or take a step back. We'll probably learn a bit more about this and become accustomed to it over time. In the same way that a fake news story from 1860 might look ridiculous to us now, we'll probably feel the same way about news stories posted in 2017 when we look back on them in 10 years. The trick is to be able to have that perspective during the moment we read the news story."

Axel Bruns, professor at the Digital Media Research Centre, Queensland University of Technology, commented, "I would expect people to have formed a considerably more sophisticated, differentiated understanding of the relative trustworthiness of different (online as well as offline) information sources."

A **principal network architect for a major edge cloud platform company** replied, "There will be more garbage in all likelihood, but its social and cultural currency will decline."

A **research scientist** said, "It will improve, and people will be more aware, and more critical."

A **senior solutions architect for a global provider of software engineering and IT consulting services** wrote, "Hopefully, the public will become more skeptical of online sources, and will gravitate toward those sources that provide more reliable and helpful information. Hopefully, people will learn to check sources online in one or two ways rather than relying on the top search result or most 'liked' item."

A **librarian based in North America** said, "People will get smarter about the internet by then. Most of the older folks who don't know the difference between clickbait blogs and real newspaper sites will die or be out of power, and people who have grown up in the environment and have digital literacy will be in charge. It's the responsibility of teachers, librarians, etc., to teach these skills to students NOW so that when they grow up they are information-literate."

A **professor at a major U.S. state university** wrote, "Not sure about the trustworthiness of information, but at least, people will be better trained by 2027."

The **managing editor of an online fact-checking site** replied, "There will be a way to parse out real from false by 2027. People always do adapt. It's just important to do it quickly."

Rich Ling, professor of media technology, School of Communication and Information, Nanyang Technological University, said, "Society faced somewhat similar issues with the development of the printing press. In that case, there was the development of mechanisms that worked to enhance to positive sides of the development while hindering the negative effects. That interaction took many decades (and perhaps centuries) to work out. Hopefully we will be able to address this issue in a reasonable way on a shorter time-scale."

There will be a divide between the savvy and the not-so-savvy, and noisy, manipulative attention-grabbers may drown out the voices of veracity

Amidst the responses there was much discussion about the likely widening of the divide in the information environment between the most educated and sophisticated members of the public who take the care to seek the most reliably sourced information and those who were not as likely to do so. Creating a "trust divide" and possibly lowering the efficacy of public discourse in maintaining a strong, well-informed public able to competently participate in creating the best future possible for all in what appears to be a struggling and contentious political system.

Alan Inouye, director of public policy for the American Library Association, commented, "I am concerned about differential impacts. More-affluent people with graduate education will continue to access systems that are mostly trustworthy. Other socio-economic groups could be subjected to less-robust systems, and importantly, the gap between the haves and have-nots grows – it is a new kind of digital divide – the trust divide."

Giacomo Mazzone, head of institutional relations for the World Broadcasting Union, replied, "The world will be divided in do-knows and don't-knows. Only the first ones will be able to find trusted sources."

Henning Schulzrinne, professor and chief technology officer for Columbia University, said, "There will be two worlds – one world of people and institutions that value factual accuracy, with correction and reputation mechanism, and the other where anything goes. The hard part is not distinguishing truth from malicious fiction but choosing to ignore the latter."

A **retired local politician and national consumer representative** replied, "Educated people will become more circumspect and select information sources they trust. The majority will believe anything they chance upon."

James Schlaffer, an assistant professor of economics, commented, "People will adjust to the amount of available information better. Also, the people who only want news from their worldview will double down on their own narratives."

Leah Lievrouw, professor in the department of information studies at the University of California-Los Angeles, wrote, "My guess is that the more popular, click-bait-y, online sources and streams will continue to have audiences (as tabloid or sensationalist, celebrity culture outlets always have). But the great online 'pool' of information will increasingly be distrusted by opinion leaders, decision-makers, institutions, and experts, who may need to create a separate 'ecosystem' of high-status – elite, if you will – and reliable sources for creating, sharing and debating information away from the populist 'roar.' Perhaps it will look a bit more like book publishing and libraries (with the 'curation' that implies), perhaps enclosed by paywalls (like academic publications?). But without an arena for trusted information to be created, circulated and debated in a fair way, there is little chance that a pluralist society can succeed into the future."

A **senior researcher and distinguished fellow for a futures consultancy** wrote, "We'll have a great array of trusted services for high-quality information. But many populations will still lack critical reading and thinking skills to discriminate between truth and fabrication."

Erhardt Graeff, a sociologist doing research on technology and civic engagement at the MIT Media Lab, said, "Most likely, between 2017 and 2027, we will see increased inequality when it comes to trust in information online and the ability of certain people to leverage the information ecosystem to serve their needs and to make change in the world. There will be elite classes who are structurally positioned online and offline to comprehend and to access the most reliable nodes in the overall information ecosystem, benefiting from existing social and cultural capital and resources like money, education, and advanced tools. And there will be underclasses whose information ecosystems who lack connections to diverse, trustworthy people and news sources, and/or who have simply been left behind in their understanding of improvements to their information ecosystems – their lack of trust will mean they cannot exploit this new landscape as fully empowered citizens."

Serge Marelli, an IT professional who works on and with the Net, wrote, "Stupid people will believe in what they want to believe: alternate facts, lies, 'alternate media,' populist propaganda."

An **ICT for development consultant and retired professor** commented, "As it is, an educated person knows how much to trust online; the better education levels, the greater a discerning individual – so one must concentrate on internet awareness and internet education, else trust will go down."

An **internet pioneer** replied, "Knowledgeable people will have semantic Web tools to check the plausibility of information from sources of unknown quality. (If Netscape hadn't invented JavaScript, we would already have had such tools.) For the rest there will be reliable and unreliable sources online, just as there are offline."

A **professor of law at a state university** replied, "There will be balkanization. Scientific and professional information will likely continue to be of high reliability thanks to professional communities policing it, while information in the public sphere will degenerate in its veracity."

A **user-experience and interaction designer** said, "A certain less-sophisticated type of user will always mistrust what they see/hear, preferring their own echo chambers. Perhaps if this was a required topic of education (critical thinking 101) in all schools, that might improve."

Some predicted most people will be too lazy or too gullible to avoid being fooled by misinformation. A **retired senior IT engineer based in Europe** wrote, "Finding information you trust will probably be very time-consuming."

A **professor of management based at a university in the U.S. West** replied, "George Orwell described it perfectly in his novel '1984,' which turned out to be somewhat late but is now technologically within reach."

Several participants in this canvassing made references to the film "Idiocracy." An **IT director** wrote, "See the film 'Idiocracy.' It is prophetic." The story line shows the quality of American life descending drastically in the future as the majority of people gradually evolve into an uneducated, crass population of consumers led by corporate-sponsored idiots.

Ryan Sweeney, director of analytics, Ignite Social Media, wrote, "Trust in information 10 years from now relies on our actions today. If we can curb these negative trends and rebuild the marketplace of ideas, our trust in information – and each other – will vastly improve. However, if we continue our current trajectory, the film 'Idiocracy' will be reclassified as non-fiction."

A **research scientist** wrote, "Trust is being eroded by lies, and the blurring of the boundary between advertising and content. I expect online information to be reduced to entertainment for much of society."

An **institute director and university professor** said, "By 2027, trust in information will be moot. The internet will be the equivalent of the 'Jerry Springer Show' broadcast from the top of a nuclear waste dump – thoroughly toxic. People won't think in terms of trust. They'll just seek entertainment."

A **professor of media and communications based in Europe** wrote, "The mass of the population will continue to believe what they like (in God, the Market, homeopathy or fairies at the bottom of the garden)."

A **technology analyst for one of the world's leading technology networking companies** predicted that in the future it will be even more difficult for voices of veracity to get their messages heard amidst the clamor raised by the attention-snatching purveyors of controversial misinformation, writing, "It will be harder to get to the diverse opinions held among my cohort as we are less active online than other groups."

A **professor of economics based in North America** said, "As the amount of information increases people will be overwhelmed. Trust will fall."

Seth Finkelstein, consulting programmer with Seth Finkelstein Consulting, commented, "When people are bombarded with contradictory and confusing information, they often fall back on a strategy of just going with their gut feelings. While that's an entirely reasonable and understandable reaction, it's also good for manipulators. When there's much noise, only what's loud and simple gets heard. That's not necessarily what's right. Thus in the absence of dramatic changes reigning in laissez-faire capitalism, I expect trust in information overall will continue to worsen."

A **partner in a services and development company based in Switzerland** commented, "We are in a race to provide users with tools for informed trust against a trend

pushing them toward a negligent attitude. I expect a move towards *informed trust* and *informed mistrust*. There is of course a great worry that *negligent trust* and *negligent mistrust* dwarf the informed and diligent attitudes on the scale of society at large. Great upheavals are possible… possibly leading to the proliferation of violent regimes."

A **retired educator** wrote, "Collective definitions of reality must continue in one way or another for society to exist. Social dissolution is possible. Or enclaves of information hubs."

A **journalist who writes about science and technology** said, "People will be extremely wary of media, and that there will be extreme balkanization of information sources. Expect the rise of FOX Nation vs. Washington Post eggheads, etc."

Jack Schofield, longtime technology editor at The Guardian, now a columnist for The Guardian and ZDNet, commented, "News sources that distribute false information have a vested interest in discrediting more-honest news sources – for example, Fox News benefits by discrediting CNN and the New York Times. I envisage more and more sources appearing over the next decade, each putting its own distinctive spin on the news, while trying to discredit rivals in similar niches. The result could be more sources catering to fewer people, with less agreement between sources about even basic facts. Once you've discredited the old 'gatekeepers' like the New York Times, the Washington Post and the Wall Street Journal, anything goes."

Marc Rotenberg, president, Electronic Privacy Information Center, wrote, "Brands will continue to determine the public's perception of trust. But perception and reality often diverge."

Diana Ascher, information scholar at the University of California-Los Angeles, wrote, "By 2027, we'll either place little stock in the information we encounter, or we'll succumb to the Borg."

Many expect a continued fragmentation or balkanization of online information communities. A **principal research scientist based in North America** commented, "Trust within internet communities will stay stable. Trust between such communities will continue to erode." A **vice president for stakeholder engagement** said, "People will have stopped trusting the internet for general information and remain within their own walled gardens or trust communities." An **activist/user** wrote, "There will no longer be a single 'online,' there will be many official and unofficial 'onlines.' with proportionally lesser or more trust attributed to them."

An **associate professor of sociology at a liberal arts university** replied, "Information and users will be even more siloed in 2027 than they are today. The internet is not an open landscape, but a platform that increasingly consists of walled gardens of liked-minded individuals. It is difficult to imagine how the structure of incentives might be changed for both users and providers in a way that would change this fact in the next decade."

An **attorney for an online civil rights organization** said, "Trust in 2027 will depend more upon our communal lives, education, economic justice and opportunity – the kind of society we have or at least publicly aspire to – than any technological innovation that might reduce freedom of online speech."

A **copyright and free speech artist-advocate** wrote, "Our commonality will continue to decrease as we will live more and more in our own little bubbles."

Stephen Bounds, information and knowledge management consultant at KnowQuestion, predicted the following potential scenario: "By 2027, trust in science and journalism without a known personal endorsement will have continued to erode. Governments and commercial organisations will all either own or lease access to significant aggregations of on-demand media. Traditional media advertising will be all but obsolete. Instead, the 'influencers' that star in these channels will be paid to pass on information to their followers. However, since this is common knowledge, their views will be treated with suspicion (thus repeating the cycle of increasing media-savviness seen in the previous iteration of advertising through mass media).

"A small but increasingly influential band of information providers known as 'patronus' will rely exclusively on no-strings-attached support from patrons. They will pride themselves on their fierce independence and champion issues of political and social importance that receive intense focus from their followers. Their success rate will be higher than the most highly-paid political lobbyists. Patronus will often be subject to information warfare attacks and lawsuits from disgruntled parties, and will be forced to invest in countermeasures as part of the cost of doing business.

"The most successful will have a staff to vet requests for coverage by governments, scientists and commercial organisations. Only a small percentage of these requests will be covered on the 'main channels,' but additional 'side channels' for niche topics of interest will be curated and published by their staff. Five years in, a patronus will suffer a damaging hit to their reputation when a second-in-command is bribed into publishing side channel content beneficial to The Walt Disney Company. In countries that outlaw or fail to develop a patronus

culture, the shift towards authoritarianism will be marked. In the absence of reputable sources of information, citizens will tend to find a single outlet for information and consume it unquestioningly, reasoning that 'they are all as bad as each other anyway.' This will make government and corporate manipulation of sentiment easy to achieve."

New and old approaches to improving the information environment will be successful

Some respondents were hopeful that one or more solutions are likely to enhance the public's trust in online information by 2027. Among the likely remedies they suggested were more public support for good journalism, enhancements to information management or filtering systems, a clear labeling or ranking of trusted sources, and new technologies, policies, regulation and education.

Larry Keeley, founder of innovation consultancy Doblin, wrote, "Parts of it will get worse. But most of it will get much better."

Jane Elizabeth, senior manager American Press Institute, said, "The current downhill trajectory will reach rock-bottom soon and prompt more serious efforts to reverse the trend. In 10 years, we can and should be able to restore some of the trust that's been eroded."

J. Nathan Matias, a postdoctoral researcher at Princeton University, previously a visiting scholar at MIT Center for Civic Media, wrote, "In our time, people already take billions of actions every month to manage and filter trusted information. By 2027, citizen behavioral scientists will routinely test the effects of these actions at scale, developing adaptive knowledge on effective ways to support public understanding in the face of rapidly-evolving misinformation."

Nigel Cameron, technology and futures editor at UnHerd.com and president of the Center for Policy on Emerging Technologies, said, "There will have been much clarification of branded/trusted sources vs. unreliable, so there should be an increasingly healthy situation."

Michael J. Oghia, an author, editor and journalist based in Europe, said, "If Wikipedia can be used as a benchmark, I've witnessed how it went from being laughable to practically a first-stop for legitimate and respectable information gathering in less than a decade. The fact is, while there is more content available to muddy the water between fact and fiction, new technologies, policies, education and human resources are being allocated to address this issue, so I'm optimistic it will improve."

William Anderson, adjunct professor, School of Information, University of Texas-Austin, replied, "Trust will be both better defined in practice and under constant review."

Barry Wellman, internet sociology and virtual communities expert and co-director of the NetLab Network, said, "We will have better means for verifying information."

Some people put their faith in better-supported journalism and education. A **consultant** said, "People who want information they can trust will fund journalism they can trust. Trust networks and leaderboards rating trust factors will be commonplace, but there will still be those looking to hack the newer systems. As always."

The **CEO of a major American internet media company based in New York City** replied, "Trust in information will be much higher in a decade. The lack of trust is mostly the fault of old media gatekeepers who think they should determine what people see. They created the opening for Trump; the distrust in media pre-dates his rise and enabled it. The millennial generation and digital news outlets will create a new kind of trust in the next decade, based on being humble guides to help people navigate the world, who 'show their work,' and are more transparent. The old gatekeepers are in the midst of peak moralizing right now and don't realize they are part of the problem."

A **graduate researcher at a U.S. university** wrote, "There are two ways this could go. We could try to regulate or program our way out of this, which probably won't work, and you'll see a massive dip in trust in information. Alternately, we could reinvest in information literacy and teach people how to navigate this new environment on their own, give them their confidence in seeking information back along with the tools to do so well, and let people rebuild trust themselves."

Some people have faith in technological innovation or human-tech combinations. An **anonymous respondent based in North America** said, "Technologies not on the radar now will be applied."

An **author and journalist** said, "We will cede much of the work of trusted information to AI's."

A **professor based at a university in the Western U.S.** wrote, "If we think about emerging technologies such as VR and experiential spaces (i.e., spaces where audio and visual accompany taste, smell and even feeling), and if we consider these might be available in realtime very soon, then it's quite easy to imagine a public that experiences information as

it comes into existence. That could, then, give rise to a new level of trust wherein information and the experience of its creation can be simultaneously felt and shared."

A **Ph.D. candidate in informatics** commented, "Systems such as internet browsers will have information verification built into them."

An **assistant director for a digital media and learning group at a California university** said, "We will develop mechanisms that will help us assess whether information is trustworthy. We will also become more sophisticated technologically to be able to tag, share or to verify information."

Andrew Dwyer, an expert in cybersecurity and malware at the University of Oxford, commented, "We will have developed frameworks of trust recognition, with some sort of verification body that attests that this has been 'fact-checked', in similar ways to emerging organisations have now. These will be plural due to the multiple perspectives required in democracies, yet others may verify another and so ecologies of trust will emerge that individuals and societies can ascribe to."

Howard Greenstein, adjunct professor of management studies at Columbia University, said, "Systems will develop where facts and origins will be sourced, so readers know where the information originated. This will exceed hyperlinks and become more like a line-by-line 'pedigree' for articles. Hopefully these will create incentives to work with the most accurate sources."

Alexander Halavais, associate professor of social technologies, Arizona State University, said, "We will see the development of metrics for determining the validity of news and information sources. This is a problem that we have already approached in search, with the need to filter 'real' responsive search results from attempts at spam or other misleading information. There is value in finding trusted information, and I suspect that people will seek ways of extracting that value, by certifying or rating the validity of claims. Unfortunately, as we have seen with Politifact and Snopes, not everyone will agree about who those certifying authorities should be."

A **director of civic technology** said, "It will be commonplace for major social media platforms to employ teams to take on propagandists, just as they employ teams to fight spam. It will be slightly more burdensome to speak online, as automated systems proliferate."

Eric Burger, research professor of computer science and director of the Georgetown Center for Secure Communications in Washington, DC, replied, "One could expect to see reputation brokers, be they private enterprise (e.g., in the U.S.) or the state (e.g., in China)."

An **eLearning specialist** said, "It seems likely that – by repeatedly proving to be untrue – the misinformation and the sources that promote it will be proven unworthy of public trust."

Maja Vujovic, senior copywriter for the Comtrade Group, said, "Trust will gradually diminish in the short and medium terms, necessitating that new filtering mechanisms be devised, tested and applied. The solutions will not come from governments, but from technology and mass human effort, akin to Wikipedia. Many people – those who can afford to – will opt to pay for access to reliable information. But the sheer number of those who cannot, coupled with ethical considerations, will spawn technological solutions and new standards in information quality control. The whole society will need to step up and this will result in a new norm of what it means to be literate."

William L. Schrader, a former CEO with PSINet Inc., wrote, "Much like HTTPS helped provide perceived improved security for financial and other information, I suspect other technologies and organizations will be created which validate that the 'publisher' is of very high or very low repute. That report can also be hacked, but it will be noticed, and published. In short, there is so little trust in online information now that trust may actually go up."

Joshua Hatch, president of the Online News Association, said, "Trust will be improved, as there will be more-sophisticated consumers and more social awareness, but the problem won't be completely solved."

Jim Warren, an internet pioneer and open-government/open-records/open-meetings advocate, said, "Trust will improve. It already has – e.g., the recent election results in England and France. Most people adjust fairly quickly to discounting false and misleading information once they recognize it as such. The trustworthiness of information will be judged in the future, as it has always been – by the reputability (in the eye of the beholder) and competency of the source."

Wendy Seltzer, strategy lead and counsel for the World Wide Web Consortium, replied, "The important thing will be the end-to-end nature of trust: Can we add enough source-to-reader indicia that enable readers to determine whether to trust the source and its reliability?"

Micah Altman, director of research for the Program on Information Science at MIT, commented, "Reaching an equilibrium by 2027 is unlikely, and advances in technology will yield cycles in information trustworthiness as technologies for manipulating and verifying (respectively) information advance, and society reacts to them. In the mid-term, distributed ledger technologies (e.g., blockchain) will provide a powerful tool for establishing verifiable information in some scenarios. In addition, as a result of trends in information privacy in Europe, trust in the management of personal information online may be improved."

The **dean of a major university's school of information science** commented, "Things will improve if there is a systematic effort to promote information literacy."

A **futurist and CEO** said, "International standards and protocols will help, and broad ethical frameworks like the Earth Charter and the UN Principles of Responsible Investing will be recognized and enforced."

Jennifer Urban, professor of law and director of the Samuelson Law, Technology & Public Policy Clinic at the University of California Berkeley, wrote, "It seems unlikely that we will get much better at discernment on an individual level. But online services may become better at sifting some information out, and we may have come up with a way to better scale our legal system's protections against false information."

A **lead experience strategist** predicted, "There will be multiple offerings for protection of identity services, and, ideally, open-source-based options that major vendors (Google, Amazon, Apple) support, based in blockchain or beyond."

Andreas Birkbak, assistant professor, Aalborg University, Copenhagen, said, "There will be more online brokers of information around who rely on a reputation of trustworthiness to attract an audience."

Rob Atkinson, president, Information Technology and Innovation Foundation, wrote, "Trust will increase by 2027, as technology improves and as more people are better able to differentiate real from fake information."

John King, professor, University of Michigan School of Information Science, said, "Caveat User: We'll learn a lot about trust, which we think we understand now, but we don't."

Stowe Boyd, futurist, publisher and editor in chief of Work Futures, said, "I predict a rapid increase in 'information trust' online that will directly track the rise in capabilities in AI. Of course, we have to trust the AIs too. Quis custodiet ipsos custodes?"

Larry Diamond, senior fellow at the Hoover Institution and FSI, Stanford University, wrote, "I will only predict, given the speed at which things are moving technologically, that by 2027 cyber technical means and consequent social and political challenges will have emerged that we haven't even imagined today."

Dan Gillmor, professor at the Cronkite School of Journalism and Communication, Arizona State University, commented, "If we do this right, people will be better able to sort things out for themselves, using critical-thinking skills and new tools that will be developed to help."

Many people who hope for solutions also question the likely success of them.

An **author and journalist based in North America** wrote, "Can third-party information be certified, trust-filtered, authenticated? Could there be systems? Would there be competing certifications?"

A **professor and researcher based in North America** said, "I don't think we will see confirmation bias or conspiracy theories go away. Trust in information will depend on trust in institutions."

A **retired university professor** said, "There's way too much hacking going on (thanks to the NSA's irrational belief that only they are smart enough to use their backdoors) for any sensible person to trust online information to be really secure or accurate."

A **founder and research scientist** commented, "Trust in information will, perhaps, be improved, but improving the overall quality of information doesn't do anything to address our natural human shortcomings (heuristics, biases, and the effects of information overload)."

Nick Ashton-Hart, a public policy professional based in Europe, commented, "Trust will increase, but the processes that increase it will also reduce the ability of new forms of information dissemination to become publicly accessible as the costs of compliance reduce the ability of the private sector, especially SMEs, to innovate."

Edward Kozel, an entrepreneur and investor, replied, "There will be fragmentation of 'trusted ecosystems' as national interests (countries) all struggle with the issues in different ways."

An **anonymous respondent** wrote, "Trust in information will go (has gone) the way of trust in advertising. People will more and more rely on input from each other. And it's not just online. Scientific research results appear one week, get discredited the next. There's incentive to be first, regardless of accuracy. That's all connected to capitalism, competition and to many social values in the United States."

Methods adopted to potentially improve things will cut free speech and elevate surveillance, changing the nature of the internet; the actors responsible for enabling change profit from control

Requiring a higher level of accountability for the sources of online information is expected to kill the ability for anonymity. A **research scientist from Latin America** replied, "Every piece of work will be untrustable unless a chain of signatures and validations can be traced to the origin." And a **professor** said, "Information can only be trusted if its full provenance is proven to be trustworthy."

This is seen as likely to stifle some needed anonymous free speech or drive it to underground spaces.

A **journalist** wrote, "A likely scenario will be that we will have better tools and systems in place to combat fake news and false information. However… the free and open net that we know today could be history due to the end of net neutrality, massive and invasive surveillance of everything happening online, one or two dominant online players such as Facebook 'eating the web,' people abandoning the web for native apps due one of these things (massive surveillance, end of net neutrality), et cetera."

A **leader of internet policy based in South America** argued, "It will be the death of privacy online."

An **internet security expert based in Europe** predicted people who wish to avoid this will have to travel the Dark Web, "The all-pervasive nature of surveillance will lead to an underground shadow IT with nobody as a recognised administrator."

Tom Worthington, a lecturer in the Research School of Computer Science at Australian National University, commented, "We may see subscriber-based services for information verification replace 'news' services. There is a risk that governments will try to regulate and force their neighbors to also do so, as Saudi Arabia is currently doing to Qatar."

Frank Odasz, president, Lone Eagle Consulting, wrote, "By 2027, we'll have learned the public internet has been soiled, and walled gardens are necessary to separate those who desire to build trust and a better world from those who seek to destroy what others have built, and/or seek to profit at the expense of others. A reputation economy is evolving where it matters what you put online (and then can't delete). But history teaches us that civilization has cycles, and we're seeing a seeming loss in America of decency, ethics and honesty and the world sees mercenary interests are in control that threaten civil society at all levels."

Some said platform companies will not work in favor of the alleviation of misinformation, instead supporting the "comfort" of online echo chambers. A **postdoctoral scholar at a major university's center for science, technology and society** predicted, "There will be a further consolidation of power in the online landscape, where relatively few companies control much of the content online. We are already well on the way to this future, with just a few companies accounting for most online traffic. 'Trust' is not currently a priority for these companies, and given the market for untrusted but comforting information, the trust environment online will continue to deteriorate."

Jason Hong, associate professor, School of Computer Science, Carnegie Mellon University, said, "There will be less trust overall by 2027 for two reasons. First, fake news is like Gresham's law: the bad drives out the good. As there is more of it, it becomes harder and more time consuming to differentiate between the good and the bad. The second is the growing criticisms (some justified, much of it not) of mainstream media. In both cases, it is important to remember that there are specific groups that benefit from both of the above (fake news and criticizing mainstream media), and thus have strong incentives to keep doing more. Unless we can find ways of undercutting those incentives, fundamentally changing the cost-benefit, we'll just keep seeing more and more fake news and misinformation."

Jim Hendler, professor of computing sciences at Rensselaer Polytechnic Institute, commented, "There will always be grey areas, but current systems that reward people who make up stories from whole cloth for political effect (via site hits and advertising, for example) must become illegal acts – stating an opinion is protected speech and should continue to be – spreading lies as truth has always been regarded as an unethical act, and current systems that reward, rather than punish, such acts are clearly eroding trust."

A **researcher of online harassment who works for a major internet information platform** replied, "It's extreme in either direction – in one direction, we're totally fine and in another, we're totally ******. If I err on the side of optimism, we can create spaces that facilitate media education, that move us away from solely SEO-driven initiatives that serve up content. I think we can make this better, but it would require really putting pressure on social networks to work with us, outside of governmental legislation."

Eugene H. Spafford, internet pioneer in cybersecurity and professor at Purdue University, commented, "Trust will become more bimodal – some sources will be more trusted as correct by the majority but a significant percentage of people will continue to view dark conspiracies and fringe theories, thus disbelieving the better sources. This will be unevenly written globally, with some countries more prone to such fringe beliefs."

Alexios Mantzarlis, director of the International Fact-Checking Network based at Poynter Institute for Media Studies, commented, "It is impossible to know. To give but one number: 10 years ago Facebook had 58 million monthly users; it now has 2 billion. Shouldn't we expect an equally dramatic evolution in our online information landscape in the next 10 years?"

Despite some attempts to improve things, things, there won't be much change by 2027

A share of respondents said the level of trust in 2027 will be about the same as it is in 2017.

Michel Grossetti, research director, CNRS (French National Center for Scientific Research), commented, "There will be a competition between the true and the false, as always."

Filippo Menczer, professor of informatics and computing, Indiana University, said, "There will be a continuous arms race between increasingly sophisticated abuses and countermeasures. Trust will not be completely restored nor completely lost."

Ari Ezra Waldman, associate professor of law and New York Law School, wrote, "Like today, people will trust information that confirms their biases. They will not trust information that challenges those biases."

Kenneth R. Fleischmann, associate professor at the University of Texas- Austin School of Information, wrote, "ICTs will continue to evolve and multiply. Fora for sharing and

receiving information will continue to multiply. Fragmentation of discourse and development of filter bubbles will likely continue to increase. It's never safe or a wise idea to predict the future, but I see no reason (apart from some kind of nationwide or global catastrophe) that our political and information environments would become less fractured and polarized over the coming decade."

Brian Cute, longtime internet executive and ICANN participant, said, "Users will have more tools that offer trust in information online. At the same time new techniques to deceive or promote fake news in new forms will be developed. It will continue to be a 'mixed bag' of trust and deception with individual responsibility being the most important element to protect the user."

George Siemens, professor at LINK Research Lab at the University of Texas-Arlington, commented, "Within a decade, the amount of misinformation will increase due to bots and propaganda, but so will mechanisms to intentionally identify and isolate false information."

A **research professor of robotics at Carnegie Mellon University** wrote, "Most people will have a few sources that they trust, inherently, but they will continue to use other, unverified sources to support their inherent biases."

A **senior research fellow based in Europe** said, "Trust online will always reflect broader trends in society, which is to say, increasing disintegration and inequality. There will always be critical, information-savvy people, but the policy arena will revolve around the majority of people who actually lack media literacy."

A **research psychologist** commented, "There will be a wide variety of trustable and not trustable sources."

David Weinberger, writer and senior researcher at Harvard's Berkman Klein Center for Internet & Society, said, "At best, we will have learned that while the Net looks like a publishing medium, it is not. It is a conversational medium in which ideas are promulgated without always having been vetted. We will become more 'meta' in our approach and recognize that we have a responsibility to question the truth and validity of what we see. That's always been our obligation but we have spent centuries outsourcing it to authorities. By 2027, perhaps we will recognize that it's up to us. It is the most basic and urgent of collaborative tasks the Net requires from us. Taking this meta step would be a significant achievement in the history of civilization. Maybe we'll get there."

A **CEO and advisor on many technology projects** wrote, "Trust will be facilitated by technologies, yet those who would subvert it will also increase efforts to defraud. It's a persistent Sisyphean battle."

Mark Bunting, visiting academic at Oxford Internet Institute, a senior digital strategy and public policy advisor with 16 years' experience at the BBC, Ofcom and as a digital consultant, wrote, "Trust in information online will be largely what it is today – that is, most people have trust in most of what they consume, but they trust some sources more than others, and can occasionally be fooled. The big question is whether trust in information from public institutions will have improved or declined – if the latter I fear our polities will be in an even direr state than they are today."

A **futurist based in North America** said, "It is unlikely that any rules would be adopted and enforced globally – and these are the only rules that could eventually help."

A **media director and longtime journalist** said, "People will move on from current trust issues/opportunities/liabilities to new ones. BUT data validation will be much easier to perform."

An **anonymous respondent from the Berkman Klein Center at Harvard University** said, "As in any society where the channels of information become suspect, a portion of the population will look elsewhere for its information. Another portion will simply refuse to process information it receives through public channels, considering all of it to be contaminated by definition. And a remaining portion will continue to believe only in the information it finds which aligns with the opinions they've already formed."

A **researcher based in Europe** said, "It will be a chain of trust, and people will trust whomever they want."

A **content manager and curator for a scientific research organization**, commented, "It will be about the same."

An **internet pioneer/originator** said, "In 2027 there will be an expanded version of what we see today: Competing, conflicting worldviews that are at war with each other in the most fundamental ways."

Taina Bucher, associate professor in the Centre for Communication and Computing at the University of Copenhagen, commented, "The next decade will see an increase in public

awareness and debate over issues of trust and information online… We all have a job to do, the public, the politicians, the technologists and the journalists alike. There has not been a better time for the humanist, social scientist and the software developer to meet."

Dave Burstein, editor of FastNet.news, said, "The best but unlikely outcome would be for people to learn to be less trusting."

A selection of additional comments by anonymous respondents:
- "Hopefully by 2027 we will begin to create institutional mechanisms for managing and rebuilding trust."
- "People will lose trust in each other because each subgroup will lose the capacity to believe and understand the other."
- "I hope people will be appropriately skeptical of everything."
- "There will be more mechanisms for redress."
- "There will be certified sources."
- "It is impossible to peer review everything."
- "Standards of verification will be even more politicized than they are now."
- "If there is a proliferation of services to vet the 'truth' – that will just further add to the information noise we already have."
- "Being 'online' will shift to the point that this question is irrelevant."
- "We will see the emergence of subscription e-systems."
- "Today's problems are yesterday's problems with speed and greater impact. We need to ask more questions."
- "Individuals will figure this out for themselves. I know I will."
- "All trust – in information online, offline, in person, et cetera – all will be eroded."
- "People trust what they want to hear."
- "People will continue to have different views of what is happening. This is the human condition."
- "Trust will be in total disarray."
- "Trust will increase for both true and false online information."
- "There will be less trust, which is a good thing."
- "There must be a concerted effort to find common ground to rebuild trust. Identity politics, intersectionality and the like are extremely divisive."

Acknowledgments

This report is a collaborative effort based on the input and analysis of the following individuals.