Pew Research Center

FOR RELEASE JUNE 6, 2017

The Internet of Things Connectivity Binge: What Are the Implications?

Despite wide concerns about cyberattacks, outages and privacy violations, most experts believe the Internet of Things will continue to expand successfully the next few years, tying machines to machines and linking people to valuable resources, services and opportunities

By Lee Rainie and Janna Anderson

FOR MEDIA OR OTHER INQUIRIES:

Lee Rainie, Director, Internet, Science and Technology research

Janna Anderson, Director, Imagining the Internet Center, Elon University

Dana Page, Senior Communications Manager
202.419.4372
www.pewresearch.org

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, collect and analyze the data.

The Internet of Things Connectivity Binge: What Are the Implications?

Despite wide concerns about cyberattacks, outages and privacy violations, most experts believe the Internet of Things will continue to expand successfully the next few years, tying machines to machines and linking people to valuable resources, services and opportunities

Connection begets connection. In 1999, 18 years ago, when just 4% of the world's population was online, Kevin Ashton coined the term Internet of Things, Neil Gershenfeld of MIT Media Lab wrote the book "When Things Start to Think," and Neil Gross wrote in BusinessWeek: "In the next century, planet Earth will don an electronic skin. It will use the internet as a scaffold to support and transmit its sensations. This skin is already being stitched together. It consists of millions of embedded electronic measuring devices: thermostats, pressure gauges, pollution detectors, cameras, microphones, glucose sensors, EKGs, electroencephalographs. These will probe and monitor cities and endangered species, the atmosphere, our ships, highways and fleets of trucks, our conversations, our bodies – even our dreams."

He was right. Today, 49% of the world's population is connected online and an estimated 8.4 billion connected things are in use worldwide.

The Internet of Things (IoT) is in full flower. The expanding collection of connected things goes mostly unnoticed by the public – sensors, actuators and other items completing tasks behind the scenes in day-to-day operations of businesses and government, most of them abetted by machine-to-machine "computiction" – that is, artificial-intelligence-enhanced communication. The most public items in the burgeoning IoT are cars, voice-activated assistants, appliances and other home systems, physician-prescribed or recommended health-monitoring devices, road sensors, public-safety and security devices, smart meters and personal fitness and health trackers for people and animals – dogs, cats, horses, cows and more. And then there are emerging IoT products that show how the urge to create connectivity extends to such prosaic items as toothbrushes, dental floss, hairbrushes, pillows, egg trays, wine bottle sleeves, baby monitors and changing tables, silverware, umbrellas, all manner of toys and sporting goods and remote-controlled pet food dispensers, to name a few.

The very connectedness of the IoT leaves it open to security and safety vulnerabilities. Every connected thing is susceptible to attack or misuse. In September 2016 at DEF CON, one of the world's largest security conferences, 47 vulnerabilities affecting 23 IoT-enabled items (door locks, wheelchairs, thermostats and more) from 21 manufacturers were disclosed. Soon after, there was a massive distributed denial-of-service (DDoS) attack on Oct. 21, 2016, against Dyn, an internet

performance management company. The attack was accomplished when tens of millions of IoT-connected devices like printers, DVRs, cable set-top boxes, webcams and baby monitors were used to launch the DDoS and block Dyn's ability to connect internet users to the web addresses they hoped to access, such as Twitter, Amazon, PayPal, Spotify, Netflix, HBO, The Wall Street Journal and The New York Times. A simple software program called Mirai was used to create the botnet that initiated the attack.

After the Dyn attack, a report in The New York Times called the IoT a "weapon of mass disruption." While that assault amounted to nothing more than a short-lived slowdown of a large portion of the internet, it showed how vulnerable connected devices are to hacking and exploitation. In recent weeks, a ransomware attack named WannaCry affected computers in 150 countries, and its creators demanded payments from those whose computers were compromised before releasing their files. Experts pointed out how dramatically this attack highlighted the vulnerabilities of the IoT.

Researchers have been showing how easy it is to hack cars, voting machines and power plants. They have demonstrated ransomware exploits against home thermostats and exposed vulnerabilities in implanted heart pacemakers. In one paper, "IoT Goes Nuclear," analysts showed how a flaw in the design of smart lightbulbs could be used for a "bricking attack" that kills all of a city's traffic lights. Within the past year Bryan Johnson (Kernal), Elon Musk (Neuralink) and Mark Zuckerberg (Facebook's Building 8) have announced initiatives to create an effective consumer-grade brain-computer interface thus, of course, hacking a person's brain could also be a future security issue.

All of this has prompted concern among internet security experts, including Bruce Schneier, who delivered a fiery speech at the Organization for Economic Cooperation and Development's Digital Economy Ministerial Meeting in Cancun, Mexico, in June 2016. He predicted that unless technology-based businesses and governments address these problems, there might be a flight from connectivity – that is, people could start retreating offline as risks mount. "My guess is we are reaching the high-water mark of computerization and connectivity," he said, "and in a few years we are going to be deciding what to connect and what to disconnect and become more realistic about what can work. We are creating a society by which a totalitarian government can control everything. Right now it's more power to the powerful. And we are living in a computerized world where attacks are easier to create than defenses against them. This is coming faster than we think. We need to address it now. People up to now have been able to code the world as they see fit. That has to change. We have to make moral, ethical and political decisions about how these things should work and then put that into our code. Politicians and technologists still talk past each other. This has to change."

Thus, the question: Could security vulnerabilities that become evident as the IoT rolls out prompt people, businesses and government to avoid or withdraw from certain online connectivity options?

In summer 2016, Pew Research Center and Elon University's Imagining the Internet Center conducted a large canvassing of technologists, scholars, practitioners, strategic thinkers and other leaders, asking them to react to this framing of the issue:

> ***As billions more everyday objects are connected in the Internet of Things, they are sending and receiving data that enhances local, national and global systems as well as individuals' lives. But such connectedness also creates exploitable vulnerabilities. As automobiles, medical devices, smart TVs, manufacturing equipment and other tools and infrastructure are networked, is it likely that attacks, hacks or ransomware concerns in the next decade will cause significant numbers of people to decide to disconnect, or will the trend toward greater connectivity of objects and people continue unabated?***

Some 1,201 responded to this nonscientific canvassing: **15%** of these particular respondents said significant numbers would disconnect and **85%** chose the option that most people will move more deeply into connected life. (See "About this canvassing of experts" on page 36 for further details about the limits of this sample.)

Participants were asked to explain their answers and were offered the following prompts to consider:

- What is the most likely kind of physical or human damage that will occur when things are networked?
- How might governments and technologists respond to make things more secure and safe?
- Is it possible to network physical objects in such a way that they will generally remain safe for the vast majority most of the time?

Several broad assertions and assumptions underpinned many respondents' answers:

Connection is inevitable: Most of these experts argued that humans crave connectivity, and they will seek more of it due to its convenience and out of necessity because it will simply be embedded in more and more things. One thoughtful framing of this idea came from **Dan McGarry**, media director at the Vanuatu Daily Post. "Connection is inevitable," he wrote. "It's what [Terry] Pratchett, [Ian] Stewart and [Jack] Cohen call extelligence. So much of human experience is based *outside* of the human being these days, you can't be a functioning adult and remain unconnected." An **anonymous respondent** put it this way: "The stickiness and value of a connected life will be far too strong for a significant number of people to have the will or means to disconnect."

Further, these experts note there is commercial incentive to add this feature to as many gadgets and aspects of life as possible. A sharp description of this dynamic came from **Ian O'Byrne**, assistant professor of literacy education at the College of Charleston, who said, "More people will become connected because device manufacturers will make it far easier and acceptable to purchase and use these devices. In the same fashion that we added electricity to every device possible with advances in technology, manufacturers will 'add the internet' to all devices in the attempt to make them better … but also possibly sell more product. In short, more people and devices will be connected."

Connectivity has many exploitable flaws: Many respondents, including those arguing the case that more connectivity will unfold, outlined downsides to hyper-connectivity. They maintained that defects and vulnerabilities are a natural part of quickly evolving networks, and software and hardware and security responses are always a step behind. Many believe that ongoing attacks are inevitable in all networked digital systems, and there will be large-scale problems in coordinating various elements of the IoT to get them to work together. While these experts expect that living an IoT-dependent life will be scary at times and often frustrating, most do not expect this will be enough to deter most people from diving deeper into connectivity.

For instance, an **anonymous professor of information and history at a state university** explained, "People can get used to anything, and – just as with terrorism – the inevitable occasional damage from deliberate or inadvertent failures in highly networked systems will become routine. Occasional terrorism using Internet of Things connections is very likely, shutting down infrastructure, hospitals, businesses, etc. Hackers will always find vulnerabilities in highly networked systems, and technical fixes will not change that." An **anonymous professor at MIT** observed, "We will live in a world of ambivalent participation."

This new connectivity jeopardizes humans and physical infrastructure, not just communication: A recurring refrain in these experts' answers is that the IoT poses significant new problems because messing with IoT-linked devices can cause real-world damage. Schneier has described it this way: "With the advent of the Internet of Things and cyberphysical systems in general, we've given the internet hands and feet: the ability to directly affect the physical world. What used to be attacks against data and information have become attacks against flesh, steel and concrete."

Barry Chudakov, founder and principal at Sertain Research and StreamFuzion Corp., wrote, "We are witnessing the advent of what the brilliant scholar and media theorist Derrick de Kerckhove (years ago) called 'connected intelligence' – but on a scale unimaginable before the 21st century. … De Kerckhove called it a 'change of being,' which captures the breadth and depth of what is happening daily as our physical and digital objects intertwine. So not only will the trend toward greater connectivity of people and objects continue, it will continue to change boundaries and

dynamics of all sorts – personal, social, moral, political. … The IoT reality represents both huge opportunity and huge vulnerability. They go hand in hand. We cannot be proactive until we educate ourselves and continue to educate others about what is required to secure IoT and what secure IoT practices entail."

Many participants in this canvassing wrote detailed elaborations explaining their positions. 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 seven major themes that are introduced and explained below and expanded upon in sections that begin on page 40 of this report.

Seven Major Themes on the Future of the Internet of Things and Connected Life

Theme 1 **People crave connection and convenience, and a tech-linked world serves both goals well**

- It's only human to connect, and there are many advantages. It's magical, even addictive
- As life increases in complexity, convenience is the default setting for most people
- The always-online younger generation can't imagine being anything but connected

Theme 2 **Unplugging is nearly impossible now; by 2026 it will be even tougher**

- Resistance is futile: Businesses will penalize those who disconnect; social processes reward those who connect. Fully withdrawing is extremely difficult, maybe impossible
- You can't avoid using something you can't discern. So much of the IoT operates out of sight that people will not be able to unplug completely

Theme 3 **Risk is part of life. The Internet of Things will be accepted, despite dangers, because most people believe the worst-case scenario would never happen to them**

Theme 4 **More people will be connected *and* more will withdraw or refuse to participate**

- Some will embrace it and some will "opt out before it happens"
- Right now the IoT isn't that grand, so why worry either way?

Theme 5 **Human ingenuity and risk-mitigation strategies will make the Internet of Things safer**

- Effective regulatory and technology-based remedies will emerge to reduce threats
- Governments should be doing more to regulate negligent companies, punish bad actors

Theme 6 **Notable numbers will disconnect**

- Lack of trust, safety and privacy issues and more may move those with fears to withdraw
- Corporate intransigence, shortsightedness and misguided thinking create vulnerabilities
- "TMI" and less-than-stellar performance from complex tech systems will drive dropouts

Theme 7 **Whether or not people disconnect, the dangers are real. Security and privacy issues will be magnified by the rapid rise of the Internet of Things**

- Threats are likely to turn into attacks and other acts, possibly some violent
- The rise of the IoT and security concerns amplifies endangerment of and worries over civil liberties

PEW RESEARCH CENTER and ELON UNIVERSITY'S IMAGINING THE INTERNET CENTER, 2017

The following section presents a brief overview of the most evident themes extracted from the written responses, including a small selection of representative quotes supporting each point. Some responses are lightly edited for style or due to length.

Theme 1: People crave connection and convenience, and a tech-linked world serves both goals well

The vast majority of expert respondents to this research study, as well as to a previous study on attitudes about the future of the Internet of Things by Pew Research Center and Imagining the Internet, agree that the IoT will continue apace, expanding vastly in size and influence over the next decade. They say businesses expect to reap large dividends from the advancement of the IoT and that people are naturally driven to connect to other people, information and services. Further, they argue that society reaps benefits from connected infrastructure and objects – from transportation, communications and business and industrial systems to individual products and services. Additionally, as modern life becomes more complicated, these respondents argue that people count on convenience to conquer chaos and they enjoy experimenting with magical new tools. Their desire for new gadgetry often outweighs any perceived risks.

It's only human to connect, and there are many advantages. It's magical, even addictive

Robert Bell, co-founder of the Intelligent Community Forum, wrote, "Because connected life offers so many opportunities in terms of cost savings, entertainment, news and public participation, people will keep moving into it."

David Clark, senior research scientist at MIT and Internet Hall of Fame member, replied, "Unless we have a disaster that triggers a major shift in usage, the convenience and benefits of connectivity will continue to attract users. Evidence suggests that people value convenience today over possible future negative outcomes."

Jim Warren, longtime technology entrepreneur and activist, replied, "From the beginning of *any* kind of 'connectivity' between humans (both biological and corporate ;-) – from primitive Man to the present – we have almost *always* favored and pursued increased connectivity. It is the essence of society, culture, productivity, improved living and lifestyle alternatives (et al.) and *will* continue. Probably the largest deterrents to the speed and pervasiveness of its development will be largely, perhaps mostly, how much it costs its users, both financially and functionally."

Mark Lemley, a professor at Stanford Law School, commented, "There will definitely be hacks and other problems, just as there are with credit cards and financial information online today. But the

advantages of connectivity are just too great for people to forgo it. We may see greater local control over when connected devices are enabled, allowing people to turn connectivity off at will."

Peter Morville, president of Semantic Studios, said, "We have a deep need and desire to connect. Everything in the history of communication technology suggests we will take advantage of every opportunity to connect more richly and deeply. I see no evidence for a reversal of that trend."

Bart Knijnenburg, an assistant professor in human-centered computing at Clemson University, responded, "The immediate and concrete benefits of connectivity, however small, will outweigh the uncertain future threats, so people will choose connectivity over security. Insurance firms may capitalize on insuring against digital threats to physical devices. The only thing that may cause people to disconnect is a widespread terrorist attack against the digital infrastructure. Even if such an attack is inconsequential for people's TVs and fridges, it may change the narrative enough that people will disconnect."

Some respondents pointed out that people are attracted to shiny new tech tools, services, platforms and systems even at times when this could become fatal attraction. There are people of all ages who find that connectivity "is addictive," one **anonymous respondent** and others argued. **Richard J. Perry**, a respondent who did not share additional identifying details, commented, "Great damage is possible and governments and vendors will strive to improve security but will fail. Internet insecurity will be the rule, not the exception. But we are addicted and will not surrender this."

David Wuertele, a software engineer at Tesla Motors, replied, "The magical behaviors that the new devices will provide will be too strong for people to resist. Even though many of these IoT devices have no real need to be connected to the cloud, and even though connecting them to the cloud presents a real risk to people, there is not enough of a force to 'clean up' the implementations. The desire by people for these magic devices is so strong that they will sign away their own personal data as well as their families' (and sometimes their friends') data to get the goodies."

An **anonymous respondent** observed, "People are influenced by gee-whiz gizmos, frequently at the expense of safety."

As life increases in complexity, convenience is the default setting for most people

Many respondents pointed out that people generally opt for what appears to be the best route to efficiency and expediency as they adopt technology. **Paul Jones**, clinical professor and director at the University of North Carolina, optimistically predicted, "The Law of Least Effort applies to the

Internet of Things. Short of massive social and political changes, we will become more connected, more networked and happier that we are."

An **anonymous respondent** who is concerned about the downsides of connectivity responded, "People will trade their safety for convenience. They always have. They always will." And **Nathaniel Borenstein**, chief scientist at Mimecast, said, "There are few examples in human history of people making rational decisions about privacy or security."

Matt Bates, a programmer and concept artist at Jambeeno Ltd., commented, "I expect the following are and will always be true with regard to internet connectivity: *Convenience* > privacy. *Convenience* > statistically infrequent health consequences. *Convenience* > statistically infrequent financial problems. For a minority, one or more of the above will be reversed and they will stand out as oddities in an increasingly connected world (note, e.g., code and security expert Dan Geer, part of the CIA apparatus, who doesn't use a cellphone). … I think most networked physical objects are 'safe for the vast majority most of the time.' It's what happens with the aggregation of networked objects that is most concerning, and then it will usually be most deleterious to a minority of the population. There's probably no way to get around this short of not networking things. Convenience will out. Sadly."

Sunil Paul, entrepreneur, investor and activist at Spring Ventures, observed, "Convenience and 'magic' will overwhelm concerns. The history of technology is clear on this front – ATMs, e-commerce, credit cards, the list is endless."

Julie Gomoll, CEO of Julie Gomoll Inc., wrote, "Hacks and ransomware won't matter. We have those now, and very few people disconnect as a result. There will be lots of junk things – 'We need a networked thing!' will be the new 'We need an app!' There will be new kinds of hacks and attacks, and we'll figure out how to stop them. We'll discover unintended consequences, attribute them to growing pains. And we will never, ever disconnect."

The always-on younger generation can't imagine being anything but connected

A number of respondents said they expect the younger generation, accustomed from the start to trust in technology with few doubts, is likely to adopt the IoT, warts and all. **Jan Schaffer**, executive director of J-Lab: The Institute for Interactive Journalism, said youth will stay connected because they are too invested in the IoT to leave it. "Young people will continue to deeply connect until they have assets and identities that they care about and don't want to put at risk," she wrote.

Lisa Heinz, doctoral student at Ohio University, observed, "Young people are perpetually connected to each other, so much so they might not know how to exist without the internet that enables that connection. As our homes become a part of that connection in even the tiniest of automated ways, we will no longer care how it works, just that it works as expected. Thus, a mass migration away from a connected society is unlikely."

Some respondents said most younger people don't know how to live any other way. An **anonymous respondent** commented, "The individuals who will be using this technology are the teens of today. It will be second-nature for them to use and interact daily across many devices and modalities." Another **anonymous respondent** replied, "Generations now take the internet for granted. They can't cope without it."

Another **anonymous respondent** wrote, "If today's adults don't get more connected, the next generation will. To today's 10-year-old the idea of a watch that can't take basic health information is like a 20-year-old trying to understand what the hell a cassette tape is."

Theme 2: Unplugging isn't easy now, and by 2026 it will be even tougher

Many respondents made the argument that disconnecting resigns people to relative isolation and some level of deprivation. They say it is not a realistic option for most people to live this life. An **anonymous respondent** replied, "It is becoming increasingly difficult to disconnect, even in the midst of threats and distrust. To be an active, engaged member of society, it is now virtually impossible to be completely unplugged." Another **anonymous respondent** said, "There will be an increasing attempt to remain unconnected or disconnect, but it will be increasingly impossible to live that way." And an anonymous **chairman and CEO at a nonprofit organization** observed, "We will continue to become more connected without realizing our critical growing dependence."

They also made the case that the marketplace for non-connected devices will shrink in the future, often leaving consumers with little choice but to accept an IoT presence in their lives. And they pointed out that even now people are often using connected devices, tools or services without knowing they are connected. An **anonymous participant** observed, "It will be increasingly difficult to unplug, as more and more aspects of ordinary daily life are plugged in. Unplugging will require a religious level of commitment."

Resistance is futile: Businesses will penalize those who disconnect; social processes reward those who connect. Fully withdrawing is extremely difficult, maybe impossible

A number of respondents observed that the usefulness and "stickiness" of IoT platforms and services plus the corporate imperative to strive for constantly rising profits will drive IoT decision-making,

causing businesses to operate in such a fashion as to make it increasingly difficult if not impossible for people to choose to opt out and still access services and functions.

Andrew Walls, managing vice president at Gartner, replied, "The benefits of IoT to the vendors of products and services will overwhelm the objections of the few consumers who fear security issues. Pricing models will penalize those who attempt to disconnect and reward those who connect. … If IoT enhances performance against consumer variables for selection/purchase, IoT integration will expand massively."

Adam Nelson, chief technology officer at Factr, commented, "People won't be able to disconnect. Manufacturers won't build in the functionality to do it."

Mary K. Pratt, a freelance technology journalist, commented, "Even if individuals are concerned about the risks, they'll find it difficult or impossible to opt out of these connections if they want to continue with the products or services they want and/or need." An **anonymous law professor at a state university** observed, "There is no choice but to become ever more networked and connected: Capital will demand it."

Several respondents likened those adopting IoT products and services to livestock. An **anonymous respondent** observed, "'Moo,' say the cattle." And an **anonymous professor at a state university** said, "Those who want to fleece the sheep will get the sheep to come on in." An **anonymous chief scientist emeritus** for one of the top technology innovation companies in the U.S. said, "Think sheep."

An **anonymous economist at Yale University** observed, "A century ago the luddites tried [to disconnect]. They failed."

Joseph Turow, a communications professor at the University of Pennsylvania, said, "Despite hacks and privacy issues, people will feel a need to keep connected, partly because companies will reward them for doing so (or make life difficult if they don't). People will feel resigned to navigating an environment where data are key coins of exchange."

Respondents resoundingly agreed that people are already dependent upon this vastly growing network, as it enables so many systems and helps so many people in successfully getting through each day. The IoT becomes more complex, more important and more difficult to disconnect from every day.

An **anonymous respondent** said, "People will *have* to be networked, because to be otherwise will mean difficulties getting employment, health care and other services that are necessary." **Randy Albelda**, an economics professor at the University of Massachusetts, Boston, agreed: "At this point I see no way out. If I disconnect, I in effect lose my job and/or pay a lot more money and/or spend an enormous amount of time living my daily life. The toothpaste is out of the tube."

Erik Johnston, associate professor and director of the Center for Policy Informatics at Arizona State University, observed, "Trying to disconnect in the future will be increasingly difficult. Only those who are either very privileged or unprivileged will find themselves in a situation where the majority of their lives are not connected in a meaningful way. As the default becomes … to opt in (unless there is a sea change in regulation) it will be very costly and time consuming to disconnect from each phase of life. And that is for the places where they know they are connected. It would be impossible to opt out of public surveillance, the TSA [Transportation Security Administration] and many other essentials of navigating a normal life."

Michael Whitaker, vice president of emerging solutions at ICF International, replied, "The inevitable march to a more-connected life will continue unabated for two reasons. 1) An increasing amount of technology will emerge that is connected by default and the onus will be on users to disconnect (rather than connect). Most users, even if concerned about vulnerabilities, will not proactively disconnect across all of their devices. 2) The general understanding of the public related to the vulnerability of connected devices will remain low. They will be sold on the benefits (of which there are many) with few voices echoing the risks. Barring an awareness-altering event, people will generally think less and less about their connectivity over the next decade and will come to expect connectivity as the default state."

Naomi Baron, a linguistics professor at American University, commented, "The issue is less about what choices individuals wish to make than about the choices that institutions or other individuals make for them. If my bank only lets me access my account online, if my telecommunications company only lets me do business online, if my doctor only makes my lab results available online, then to disconnect from the internet would mean disconnecting from the individuals, institutions and services I need for everyday life."

Some are concerned with people in certain segments of society being unable to choose to fully or partly opt out as they wish. An **anonymous senior research scholar at a U.S. university's digital society lab** said, "Both statements are likely to be correct. Most people – the poor, vulnerable, dependent – won't have the means to disconnect. Social and political systems – education, employment, government services – will require them to stay connected. Those educated, independent and privileged enough to prioritize their rights and liberties over public systems will

increasingly disconnect or manage their connectedness. Privacy and liberty will become ever more the province of those with economic means."

You can't avoid using something you can't discern. So much of the Internet of Things operates out of sight that people will not be able to unplug completely

A number of these experts raised the point that as connectivity is becoming built into everything, people often do not know what is connected, what is collecting data, who sees the data that are collected and why, and how all of these things are linking to other things. **Andrew Walls** of Gartner said, "People will remain largely unaware of the degree of connectedness present in the products they select and will merely pick products and services based on personal preferences for comfort, convenience, value for money, etc."

Jamais Cascio, distinguished fellow at the Institute for the Future, wrote, "More people will be more deeply connected, but will likely be less aware of it. Think of it as the 'electricity' effect. It's rare today to see something called out as being run on electricity (vehicles are the main exception); we just assume that a device or building or system is electricity-enabled. The default 'guitar' is electric, and acoustic guitars must be labeled. Similarly, in this decade we'll be moving quickly into a world where networked/'smart'/internet-enabled will be the default assumption, enough so that many people will stop thinking of it as new or different. You'll have people extolling the virtues of being 'unplugged' because they don't have any computers in the house and keep their mobile devices shut off, but [they'll] forget that the household appliances and carpeting and home solar power array are all deeply networked, because they don't have to think about or worry about those systems."

Bob Frankston, internet pioneer and software innovator, replied, "A significant number will have the *illusion* of being disconnected [when they actually are not]."

Theme 3: Risk is part of life. The Internet of Things will be accepted, despite dangers, because most people believe the worst-case scenario could never happen to them

Many of these respondents point out that optimism bias generally moves people to perceive a potential risk as highly unlikely to harm them. When people ask themselves, often subconsciously, "Do the benefits outweigh the risks?" the answer is generally, "Yes – go for it!" – especially when connection and convenience are the result. The majority in this canvassing predicts that the general public expects that any problems tied to their connectedness will fall primarily upon others, not themselves.

An **anonymous computer software sales engineer** replied, "Most people aren't aware of the complexities of online security and assume it will happen to someone else."

Daniel Berleant, author of "The Human Race to the Future," said, "All change comes with risks. You don't see people moving away from cars (with occasional individual exceptions) because cars are dangerous. The dangers of using digital technologies are lower than for cars and while these dangers will be a continuing concern, they won't stop the overall digitization trend."

An **anonymous respondent** said, "People uncritically accept new things: Drones, self-driving cars, corporate exploitation, terrorist incursions are routed through the internet, control over nuclear reactors. The TV show 'Mr. Robot' is extreme and entertaining, but it is pointing to issues that are real."

An **anonymous web developer** commented, "Pickpocketing hasn't made people stop carrying wallets, has it? Unless there is a major attack, affecting literally *billions* of people … in the near future, more people will be connected. As the number of connected people grows, individual cyberattacks and fraud will probably grow as well. Increased attacks probably will not cause massive disconnect, because the positives greatly outweigh the risks."

Maria Pranzo, director of development at the Alpha Workshops, replied, "Wow. I'm trying to remember how it was before we were all connected. Before the world knew what was going on everywhere at once. It's a frightening thought, all of this going away. And yet it's one that I could be completely comfortable with. But that's my privilege showing. Online security is, by and large, an illusion. And I think we all agree to the illusion together. We count on good people on the front lines: the makers of our hardware and software. We count on their continuing to advance slightly faster than the bad guys. Most of us do so blindly. Why would that change? I certainly don't check the plane engine before I get on a flight."

Stephen Downes, researcher at National Research Council Canada, said, "It is true that attacks, hacks or ransomware concerns impact our enjoyment of modern technology. But it's important to note that what they impact is almost exclusively our enjoyment of modern technology. A person choosing to disconnect from modern technology suffers the same fate as the person who has been hacked. They lose the enjoyment of modern technology. So disconnecting from technology isn't a viable response to attacks, hacks and the rest. People won't be looking to withdraw from modern technology, they will be looking for better and more secure modern technology (to a point; as people's choices of passwords such as '123456' show, they are willing to sacrifice a certain amount of security for a certain amount of convenience. Indeed, if anything forces people off new technology, it will be the security measures, not the crimes)."

Theme 4: More people will be connected *and* more will withdraw or refuse to participate

A share of the experts in this canvassing think that the future will bring far greater connectivity for most users *and* that – at the same time – a notable number of people will cut back their ties to connected things or withdraw from that world. They also imagine scenarios where people try to modulate their level of connectivity, being embedded to some degree in the connected world and, to some degree, also withdrawing from it.

Some will embrace it and some will 'opt out before it happens'

Jeff Johnson, consultant at UI Wizards and Wiser Usability, replied, "My actual answer is 'both.' Most people will move more deeply into connected life, but significant numbers will disconnect (or remain disconnected)."

Adrian Schofield, an applied research manager, observed, "Both answers apply. Millions will connect because they are at low risk and the convenience factor is high. Thousands will disconnect because they become targets or they fear becoming targets. However, fear of losing wealth has never stopped the relentless pursuit of wealth."

Wendy M. Grossman, an independent writing and editing professional based in London, said, "As we become more sophisticated about and used to these technologies, we will (I hope) make better-informed decisions about which ones we use and how. … As I watch the way IT is developing, I'm increasingly dubious about how far I want to let it – and the concomitant exposure to potential surveillance – penetrate into my home life. Some of this is because I've been online for 25 years and I write about security – I'm distrustful enough that I do almost no online banking and don't use my smartphone for anything that would expose any of my financial accounts. I'm in the fortunate position of not needing to do these things, so I don't. I think in the short to medium term we're in for a lot of grief as legacy manufacturers who know nothing about security add wireless connections and computational power to everyday objects; there's going to be a big mess one day soon when governments start demanding that the data collected by smart TVs, robots, etc., be retained for use by law enforcement and security services. It's simpler (to me) to opt out of that before it happens."

An **anonymous employee of the U.S. National Science Foundation** wrote, "Both answers are true, since 5% to 10% disconnecting is a significant number."

An **anonymous respondent** said, "All devices will become connected by default. It will take an effort to disconnect. But more people will become distrustful of the IoT. It will cause a large culture

clash." And an **anonymous network architect** observed, "I actually think both are true, possibly resulting in a bifurcation in our social structure."

John Paine, a business analyst, commented, "There will be a statistically significant number of people who will deliberately disconnect to the extent possible, but overall connections will increase. I expect that a premium will begin to come into play for purchasing 'disconnection' as a feature for goods/services in the future."

An **anonymous respondent** replied, "The answer is both/neither/it will balance out. Many will disconnect, but equally as many will double down. For every tin-foil-hatted neo-Luddite moving to an island with a telegraph, so to speak, there will be someone gleefully enjoying their networked toaster and toilet. The only thing that might tip the balance more toward disconnection would be an IoT-related infrastructural disaster."

Right now the IoT isn't that grand, so why worry either way?

A share of respondents expressed a low level of confidence that the IoT or the security of the networks will advance much in the next decade. Those whose responses generally referred to consumer-oriented applications such as "smart-home" items tended to find them to be less than worthy of sacrifice of one's privacy or safety. They don't think IoT uptake will live up to expectations, but they generally are not considering larger systems in the IoT such as transportation, environmental services and finance.

Grant Blank, a sociologist and survey research fellow for the Oxford Internet Institute, said, "The question seems to assume that most people own devices that are part of the Internet of Things. This is currently false. People will generally stay away. There are two reasons: 1) Security is being done badly on the Internet of Things. This seems unlikely to change quickly. 2) Companies are behaving in ways that discourage participation. Major case in point is that Nest recently decided to turn off the servers supporting a whole line of devices, making devices costing $100+ into useless bricks. The bottom line is that the Internet of Things is more useful for companies than for consumers. Consumers will generally stay away."

An **anonymous** respondent commented, "I don't believe the Internet of Things will really become reality. The infrastructure is not good enough and the high number of manufacturers will create lock-ins. The threshold for citizens will be too high – unless they commit to one manufacturer and buy *everything* from it."

An **anonymous scientific editor** replied, "It's hard to know/guess which way things will go. For me personally, I back away from this stuff as far and as fast as I can, but I'm not sure how many other people will be inclined to do the same. It's entirely possible that most people will find these ridiculous and dangerous new toys irresistibly compelling. Really though, it's beyond parody. 'Smart TV'? C'mon, you're having a laugh. How might governments and technologists respond to make things more secure and safe? Well, air-gap them, obviously. Very little of this stuff ever needed to be networked in the first place. Cellphones: Good. Highway traffic flow control: Good. An app that controls the light switches in your home: Not so much. As for an automobile controlled by a computer: If it's an autonomous self-driving car a la Elon Musk, then sure, recent fatality notwithstanding; if it's a regular car, then OK, there are pros and cons for digital vs. analog; if it's a regular car with a networked computer, hell no! There's absolutely no upside to that whatsoever."

An **anonymous senior fellow at an organization that examines the future of privacy** issues replied, "People may adopt, then disconnect based on experiences. For example, I don't see the point in a refrigerator with a 21-inch display in the door, and a lot of the other IoT features seem like overkill. For sensors, horror stories about surveillance may deter use. Connected and driverless cars present challenges with the first fatal crash. It will be interesting to see what happens."

Theme 5: Human ingenuity and risk-mitigation strategies will make the Internet of Things safer

Many respondents expressed confidence in the evolution of methods by which outside regulators, as well as developers of the software, hardware and networks undergirding the IoT, will build in some method of dealing with constantly emerging security, safety and civil liberties issues.

Indeed, regulators have just started to consider recommendations in this fast-evolving setting, moving slowly and not forcefully. The Food and Drug Administration's (FDA) guidance for management of cybersecurity in medical devices was issued as a draft in January 2016 but not officially released until a year later. The recommendations are nonbinding – more like suggestions. And when the Federal Trade Commission (FTC) announced in January 2017 an IoT "Challenge to Combat Security Vulnerabilities in Home Devices" some experts worried that the top prize for winning submissions was a modest $25,000.

An **anonymous futurist** wrote, "The vulnerability of networked devices is a technical issue. The original inventors of the internet are basically good people, so they did not recognize all the ways that their devices can be exploited. As the bad actors expose more problems, they will be fixed. I expect that networked devices will become as reliable as our electric power grid today. It will occasionally go out – and it will be a catastrophe. But we will survive."

Effective regulatory and technology-based remedies will emerge to reduce threats

Pamela Rutledge, director of the Media Psychology Research Center, commented, "The advances in technology will be accompanied by improved security. That is the only way companies and organizations can protect the economic investment in connected products and services; it is the only way connected services can continue to deliver value. There will always be some who choose to self-regulate by withdrawal, but most will learn new skills of self-management and be willing to exchange the currency of personal data and privacy to get the most value from the products available."

Patrick Tucker, technology editor at Defense One and author of "The Naked Future," wrote, "Biometric authentication and IoT military research programs such as the HACMS [High-Assurance Cyber Military Systems] program will make the Internet of Things more secure. That plus new services that spring up out of the Internet of Things ecosystem will shift the cost-benefit analysis of staying engaged and deepening engagement toward deepening."

Jon Lebkowsky, CEO of Polycot Associates, said, "It's an arms race, for sure, but I'm confident that we will evolve better security. And I'm pretty sure the negatives along the way will not diminish trust to the point that people disconnect in a big way."

Michael Wollowski, associate professor of computer science at the Rose-Hulman Institute of Technology, explained how advances will allow systems to be self-monitored and self-protected. "I am not concerned about vulnerabilities of the Internet of Things," he said. "In addition to improvements of security tools [thanks] to advanced analytics devices [used in] factories will become what might be called 'self-aware,' i.e., they will 'know' when something is not right. In those cases, the devices will enter different levels of self-protection based on the perceived threat. Better communication among security experts and systems will also provide for quicker responses to threats, isolating or eliminating them."

An **anonymous respondent** commented, "It feels like an inevitability that some series of high-profile ransomware attacks, e.g., turning off an IoT pacemaker to take out a U.S. senator or CEO, will happen, because human greed is not a force we're likely to eliminate in the near term. That said, I doubt the backlash against that kind of attack will be disconnection, it'll be the solidification of security standards and 'trusted' brands of devices. There will always be both greedy bastards and the tinfoil hat brigade, but my hunch is that both sets will remain on the fringes, with the middle 90% opting to make smarter decisions about who/what has access to certain information/devices."

Governments should be doing more to regulate negligent companies, punish bad actors

An **anonymous tech ops lead** replied, "We've seen this movie before. 'Don't ever put your credit card on the internet.' 'The internet isn't secure enough for banking.' Etc. If enough people trust it, it becomes imperative to fix it, and it gets fixed. But some of the early pioneers randomly get arrows in their backs. People already share their entire lives with (fairly insecure) laptops and tablets. There is an entire antivirus industry focused on the wrong part of security. There will be many massive problems where houses, toasters, video feeds get taken over because nobody knows what is secure and what is not. But, over time, best practices will emerge (just like most sites encrypt their passwords with a salt [random data used as an additional input], but soon they will use two-factor authentication). Governments can help by making sure customers who are harmed can sue and get money from negligent companies. Toyota didn't care about software best practices, but was forced to pay a billion dollars and given a wakeup call: They are a software company now. It's best for consumers if products are self-updating. But that requires 1) trust and 2) laws. Without laws, companies would rather focus on selling a new product rather than fixing an old one. Hopefully the law will say, 'Either fix the bugs or open-source so anyone can fix the bugs.'"

An **anonymous staff member at a state university** said, "We have had great moments of mistrust, which have stemmed largely from an underestimation of threats and a misunderstanding of the network and how they work. As citizens become more educated about the network and how things are connected, more pressure will rise to provide safe and secure spaces. However, organizations that exploit the data and the network should be found and swiftly punished instead of being tacitly ignored as we see so often."

Demian Perry, director of mobile at NPR, observed, "The problem with IoT devices is not that these devices are inherently less secure, but that the space is too new to have a mature security infrastructure. The market is likely to weed out insecure products over the long term, but it might also be helpful to have regulatory review over certain product categories, similar to the way the FDA manages food safety, or the role the National Transportation Safety Board is now playing in autonomous vehicles."

Jason Hong, associate professor at Carnegie Mellon University, commented, "In the short term, we will see a lot more IoT-based attacks, especially ransomware attacks. However, organizations are already taking steps toward improving the situation. For example, the FTC has issued reports on IoT security and is asking the top manufacturers about their cybersecurity practices. Over time, I expect there to be more centers of excellence to help disseminate best practices for coding and managing IoT systems. Researchers will also come up with better ways for managing collections of devices as well as protecting low-end devices. It's also likely that insurance companies will help improve the

state of the art by having higher premiums for IoT companies that don't have good cybersecurity practices. Most importantly, cybersecurity is a known issue, and both IoT manufacturers and consumers are becoming savvier about the risks. So while there will be a lot of growing pains, I'm optimistic about the future of IoT."

Richard Forno, senior lecturer of computer science and electrical engineering at the University of Maryland, Baltimore County, said, "As a career internet security professional, I continue witnessing people rushing to embrace the latest and greatest thing or gadget or service without thinking about the possible ramifications to their security, privacy or resiliency. And it's not just about security or privacy – what if the product vendors for your IoT-enabled things go out of business or decide to make their product incompatible with others in the same space? (Which is happening already.) What will users do then? Accordingly, security practitioners and educators at all levels will constantly struggle to inform the public about these risks in ways it can understand easily and potentially address in their respective lives."

Theme 6: Notable numbers will disconnect

Some 15% of the respondents in this canvassing expect that perceived and real vulnerabilities of the IoT will move people to disconnect. They noted the escalating security and privacy risks posed by connected devices and the complications that occur when fast-changing, fast-growing complex systems are built and networked. Many among this share of respondents seem to have little to no confidence that the builders of the IoT will make security, safety and individuals' civil liberties their first priority because profit, power and efficiencies always come first, leaving far less investment in the crucial, difficult, expensive and perpetual work of minimizing threats.

Lack of trust, safety and privacy issues and more may move those with fears to withdraw

Expressions of concern, disappointment and resignation are evident in the responses from those who say it is likely there will be some who choose to disconnect in some manner from the IoT. Mistrust is the big factor in these answers, especially when it comes to other humans. Their worries are generally tied to 1) their expectation of harm from criminals and other bad actors; 2) their suspicions about the primary motivations behind the acts of the corporate and governmental bodies they must depend upon to operate these networks and 3) their lack of faith that people can get it all together to plan, regulate, build, monitor, update and maintain such complex systems.

An **anonymous senior researcher at Microsoft** wrote, "Most people will move more deeply into connected life. Then there will be some catastrophe – some enormous hack that costs thousands and [takes] lives – and then people will try to disconnect. For example, self-driving cars take off and then someone figures out how to hack them, causing an enormous loss of life in one fell swoop."

An **anonymous respondent** replied, "I expect that within 20 years it will be very difficult or impossible to buy non-IoT versions of many common items (this is already rapidly becoming the case with televisions). The current norm of poorly engineered, non-updatable, easily exploited IoT 'security' will continue, further opening the surveillance window for governments and corporations and creating an even vaster, botnet-armed cybercriminal underground."

An **anonymous respondent** said, "More, and more serious, data breaches are likely to push people away from the Internet of Things. Stalkers using home webcams to collect information, breaches of medical records that are used to blackmail thousands and subverted automobiles will drive educated consumers away from insecure systems."

Joel Barker, futurist and author at Infinity Limited, said, "Disconnection is the only solution to the size of the risk."

An **anonymous respondent** said, "Short-term [there will be disconnection]. This stuff has happened, and is happening. An electronic cold war. It might be revealed. Long-term, electricity will be a memory for most people. Have you read "The Road"? We are on that road."

Corporate intransigence, shortsightedness and misguided thinking create vulnerabilities

Jennifer Zickerman, an entrepreneur, replied, "Sadly, people will continue to connect devices without demanding better security design. Shiny new technology will trump big, dumb security vulnerabilities. Institutions are particularly vulnerable, as they stand to reap the greatest benefit from 'smart' devices. We will see situations where hospital equipment, utility systems, even entire buildings are held for ransom. It is most definitely possible to improve security – however, that would involve settling on a common, open-source security standard, which tech corporations are loath to do. (Witness the fragmentation of single sign-on systems.) As long as tech companies continue to look at security as a 'feature' rather than as a fundamental operating characteristic, they will be unable to cooperate to build proper security infrastructure. As long as society continues to allow tech companies to reap vast profits in spite of the damage they do to users through a lack of effective security, tech companies will have little incentive to improve."

An **anonymous systems engineer** replied, "Corporate greed prevents things from being done well, thus the Internet of Things is a horrifically stupid idea that will drive people back to using technology that can't be corrupted by corporate greed."

Jesse Drew, cinema and digital media professor at the University of California, Davis, replied, "There is a limit to the trust people put into their machines."

An **anonymous advocate for international freedom of expression** wrote, "I don't feel confident about the state of data security at the moment, and I fear that putting more data in the hands of reckless corporations will endanger us. Consider the impact of a leak of health-related information – what's to stop predatory insurance companies from denying coverage?"

An **anonymous chief technology officer** commented, "Until security improves, a significant number of sophisticated users will disconnect. I'm not going to install a Nest, my next TV will not run apps, even if it costs me more, and I'm not going to get a Samsung internet-connected refrigerator. I will willingly give up convenience until the developers get it right. If they ever manage to."

A call for open-source processes and standards came from **Alexander Halavais**, director of the master's degree program in social technologies at Arizona State University. "We will see the same battles we already have between closed infrastructures and open, interoperable ones," he wrote. "We are already seeing the early days of this with wearables. Your Withings devices all talk to one another, but talking across makers becomes more difficult. Services like ifttt [If This Then That] are fighting against these new walled gardens. The future of these systems requires open standards. It took a long time for web browsers and operating systems to learn this lesson, and government regulation has played a role in making such exchange even more difficult, but it is likely a question of when, not if; eventually makers will come to understand that open standards improve user experiences and lead to greater adoption."

'TMI' and less-than-stellar performance from complex IoT systems will drive dropouts

Some respondents wrote that people might simply withdraw from connectivity because they are overwhelmed. Among the contributing factors would be information overload; poorly made or overly complex IoT tools and systems; products that do not perform well, lack support and/or are in constant need of updates and patches; and IoT products that are given to new owners without the manufacturer knowing of the switch. As a result, some of these respondents say, people will disconnect to a certain degree or never consciously connect.

Timothy C. Mack, managing principal at AAI Foresight, wrote, "At present, the Internet of Things is more a series of missteps than a grand design, if for no other reason than many of the large players are competitors versus cooperators and accepted protocols are still not agreed upon. As well, the 'gold rush' quality of such areas as 'smart homes' has led to shoddy design and poor construction of the physical and the digital aspects of this brave new world. As for the loss of critical safety and security through networks trying to interconnect and protect and the same time (with largely the same tools), we should expect many more disappointments in the IoT development saga."

Ryan Sweeney, director of analytics at Ignite Social Media, commented, "We're going to see two groups start to emerge within the next decade: those connected and those unplugged. Being connected can be burdensome to users as they face information fatigue. Bret Easton Ellis wrote a book titled 'Lunar Park' that provided a fascinating take on the concept. (Spoiler alert!) Ellis depicts a world where kids are so saturated with information they become bored with and numb to technology so they run away and start a community of their own. In Dave Egger's book 'The Circle,' (spoiler alert) a character strives to escape the oppressive nature of an omni-connected dystopian future and finds death to be the only way out. Exaggerated? Yes. Conceptual plausibility? Definitely. Meanwhile, as algorithms become more efficient and technology more omnipresent and accepted, there will be continued growth of plugged-in users. Governments will need to focus on protecting the connected user, as acts of terrorism will likely shift to the digital when the damage potential is great enough. When everything is connected and relies on said connectivity of other sources, disconnecting one system could result in a significant freeze of efficiency. If, for instance, within this decade automated cars become standard that system could become compromised resulting in anything from an economic shock to massive loss of life by collision. The sci-fi nerd in me wonders if, in several decades, this will result in a new type of class system."

Pete Cranston of EuforicServices.com said the machines will manage the complexity, observing, "There will be scares, genuine disasters, but the potential gains from interconnectivity are so great that we will continue to lurch into a future where we will have to confront issues of independent machine-machine decision-making (aka machine intelligence, but actually more to do with interlocking algorithms exponentially increasing the complexity of machine response patterns) much more actively."

Theme 7: Whether or not people disconnect, the dangers are real. Security and civil liberties issues will be magnified by the rapid rise of the Internet of Things

Many respondents to this canvassing said the dangers of the IoT are real and present a daunting challenge. They are certain that in the future there will be more attacks with more devastating results as billions more things and people become interconnected online and systems become more complex and difficult to manage. Many have deep concerns about the protection of civil liberties in a world in which so much granular data is continuously collected and databased, especially considering the fact that the "threat environment" created by this complex networking is high.

Threats are likely to turn into attacks and other acts, possibly some violent

An **anonymous engineer at Cisco** commented, "It is inevitable that more people will be connected more and more, but we do not expect the security, which is a cat-and-mouse game, to

significantly improve relative to the number of things getting connected. People will lose their lives due to criminal exploits of vulnerabilities."

An **anonymous programmer and data analyst** wrote, "Most people are totally oblivious to the fragile and easily pierced nature of the Net and the total lack of protection of their medical/financial information. They will continue to not care or understand the issues and will move more deeply into connectivity. Attacks on power infrastructure, automated vehicles, airplanes, food supplies are all unfortunate consequences of the IoT."

Jerry Michalski, founder at REX, replied, "Aside from climate change and clowns having their fingers on the nuclear trigger, the IoT is one of the larger menaces we face. Any device that's been in the field over five years is highly likely to be p0wn3d [a gamer term meaning "beaten handily"] by the darknet. All of which sounds like I should have answered that people will withdraw from the IoT, but within the next decade I believe people will just dive in merrily, because we're in the uptake period of this new technology and the big flaws won't show up within the decade. We would do well to rethink entirely the structures of the vaunted Internet of Things."

John Howard, creative director at LOOOK, a mixed-reality design and development studio, commented, "The growth of IoT, along with 3D printing and VR, will further erode the digital/physical divide. Physical peril (real or imagined) will put greater emphasis and opportunity on network security. … As physical attacks become more public, people will understand the need to take greater responsibility for their own cybersecurity."

The rise of the IoT and security concerns amplifies worries over civil liberties

Some respondents expect that because the risks associated with the IoT are high, that will compel greater surveillance by governments. Advanced artificial intelligence tools will be able to monitor, analyze and pass judgment upon nearly every detail of any individual's life via the data collected by the IoT. Sentiment analysis can be applied to create a profile of people's character and intentions; experts say such programs will enhance security and endanger civil liberties. A number of these experts worry that those who control the algorithms will begin to even more deeply exploit the constantly multiplying ways in which they can monitor users' behaviors and emotions and even predict and/or manipulate how people behave. Some experts say if the brain-to-internet interface were to become a reality, this type of spying could possibly capture and process human thought. It is a sci-fi nightmare brought to life. An **anonymous respondent** described a worst-case scenario, writing, "It's the tragedy of the commons: The individual incentives are great (better health, more convenience, saving money) while the long-term consequences for society are grave (loss of privacy, autonomy, safety in one's own home)."

Marti Hearst, a professor at the University of California, Berkeley, replied, "Just as the pervasiveness of cellphones forced the phasing-out of pay phones in public places, it will become impossible to opt out of the oncoming connected world. People's businesses, homes, cars and even their clothing will be monitoring their every move, and potentially even their thoughts. Connected cities will track where and when people walk, initially to light their way, but eventually to monitor what they do and say. The walls of businesses will have tiny sensors embedded in them, initially to monitor for toxins and earthquakes, and eventually to monitor for intruders and company secrets being shared. People currently strap monitors on their bodies to tell them how many steps they take. Eventually, all fluids in and out of bodies will be monitored and recorded. Opting out will be out of the ordinary and hugely inconvenient, just as not carrying a mobile device and not using a fast pass on the highway are today."

T. Rob Wyatt, an independent network security consultant, wrote, "Functionality trumps lack of security every time. We develop new function almost without regard to security and then discover we cannot retrofit it after the fact. A recent court ruling stated that we should no longer have any expectation of privacy in our internet-connected devices. Considering that we now have forks, toothbrushes, health monitors, mattresses, sex toys and more connected to the internet, this ruling has profound implications to personal life, privacy and checks and balances to government intrusion and control. The ruling went almost unreported and no public outcry was raised over it. No public backlash will occur so long as the toys are shiny."

An **anonymous respondent** observed, "It is a huge invasion of privacy. The Internet of Things is not something I want to participate in fully. Only in very limited ways that I can control. But I am older, and wary. Younger folks who have grown up with technologies may not care, so interconnection will grow. I'm still going to buy a TV monitor without a camera, because I don't want that part of my life camera-enabled. I don't want my fridge enabled. I don't really want much of anything enabled. I want privacy."

An **anonymous computer science professor at a Swiss university** wrote, "The main issue with connected objects is the potential to trace people, their actions and activities, or to hack objects and change their behavior. We should *avoid* having completely centralised systems where each event is recorded and sent to governments or surveillance bodies."

Mary Chayko, communications and information professor at Rutgers University, replied, "While cybersecurity has become a critical challenge for governments, psychological security – a sense of safety and rootedness – becomes perhaps the premier challenge for individuals. As we see our devices and world become ever more tightly networked and interconnected and recognize the inherent security vulnerabilities in such a system, we become more psychologically and emotionally

vulnerable. My hope is that we will address this, as we have so many other issues in the digital age, in community with one another – coming together (often online) to better understand our common human responses, needs and frailties, and to develop stronger, more secure systems and selves."

Responses from additional key experts regarding the future of connectivity in the age of the Internet of Things

This section features responses by several of the many top analysts who participated in this canvassing. Following this wide-ranging set of comments, a much more expansive set of quotations directly tied the seven primary themes begins on page 40.

'Whose intelligence? Whose control? … How can we monitor the monitors?'

Barry Chudakov, founder and principal at Sertain Research and StreamFuzion Corp., replied, "We can now unleash the power of all brains, all consciousness – both somatic and artificial – to solve problems and improve the human condition. This is truly a remarkable development. … Bruce Schneier says the Internet of Things, with the computerization of everything, will be the world's biggest robot. This everything-everywhere 'robot' – a concatenation of connected things, sensors and actuators – will change the world in ways we cannot predict and will maximize profits for those who control the components. Physical or human damage might be contained … or it could leave nations and governments more vulnerable to hacktivism and cyberterrorism targeting air monitoring, water and electrical infrastructure systems. … Smart and networked also means malicious actors can hack these systems and create mischief and worse. … The Internet of Things is a way of not only connecting objects, but also embedding intelligence into those objects. That intelligence is persistent and will soon be ubiquitous. Very quickly the question arises: How much intelligence? And how much decision-making, or control, can be embedded into those objects? … The mostly likely physical or human damage that will occur when things are networked arises in this area: Whose intelligence? Whose control? How do we, if need be, circumvent it or turn it off? How can we monitor the monitors to ensure no bad actors are trying to harm us using IoT as a weapon?"

Fixes will arise because the cyberphysical space is the fastest-growing part of the economy

Glenn Ricart, Internet Hall of Fame member and founder and chief technology officer of U.S. Ignite, said, "There is tremendous latent potential in greater connectivity – enough potential to force providers and consumers alike to find ways of minimizing the inevitable downsides. Just as Underwriters Laboratories (the famous UL label) was started by insurance companies to minimize losses due to fire and other malfeasance of new electrical technology, I would expect that organizations like Mozilla and Electronic Frontier Foundation and others will create testing

programs and labels that will have value in creating trust and reducing vulnerabilities. At some point, the National Institute of Standards and Technology will find that it must turn the majority of its activities to standardization and testing in the cyberphysical space because that is the portion of the economy growing most rapidly."

'The attacks will get much worse' but there are 'ways to mitigate them'

Cory Doctorow, writer, computer science activist-in-residence at MIT Media Lab and co-owner of Boing Boing, said, "The attacks will get much worse. There are a variety of ways to mitigate them. First, in the line of establishing more graceful failure modes: Eliminate Section 1201 of the DMCA [Digital Millennium Copyright Act] and the Computer Fraud and Abuse Act, both of which are routinely used to suppress true facts about security defects in products we rely upon. The current model is that we learn about these facts not when they're discovered by a 'good guy' but when a 'bad guy' exploits them so horribly that their existence can no longer be suppressed. Second, use legislation to force firms to internalize the cost of breaches: Right now, losing a credit card record costs a firm something like $0.35, plus a six-month gift certificate for a credit-monitoring service. But the data from those breaches, combined with other breach data by crooks, can be used to pull off breathtaking identity theft crimes (last Christmas saw a rash of thefts of *whole houses*, accomplished by assembling enough identity data to successfully procure duplicate titles/deeds). If firms had to pay the entire likely lifetime losses from breaches (because of statutory damages and/or precedents) then no insurer would underwrite companies that were as sloppy as today's – data collection and retention would be priced accordingly by insurers, at a much higher price than today's. (Today, the major expense is hard drives, not liability insurance for all that potentially explosive material.) Third, eliminate the state mandates for collection and retention, especially those in the European Union, which press firms into service as proxies for law enforcement, and which simultaneously mandate the mass collection/retention of sensitive PII [personally identifiable information] that will eventually leak and be exploited by crooks."

A better evaluation and certification system for devices is needed

Henning Schulzrinne, professor at Columbia University and Internet Hall of Fame member, commented, "Consumers currently have no reasonable way to judge whether the devices they buy are designed according to common security practices, whether and how they are being tested, how security-related bugs are addressed and for how long after purchase. Nor do they generally know what kind of data the vendor stores where, shared with whom and for how long, and whether those systems are regularly tested by independent third parties. For higher-risk devices that can either do physical harm (cars) or can cause significant loss of privacy (in-home cameras) or endanger physical safety (door locks), some kind of certification that does not just consist of 10 pages of disclaimers seems necessary."

Technology has always inspired fears, but 'people found ways to use them effectively'

Jonathan Grudin, principal researcher at Microsoft, observed, "Previous hardware generations and major software advances gave rise to fears, but people found ways to use them effectively, warranting measures to prevent serious misuse or negative consequences. Why would this be an exception?"

People will demand solutions to problems in the cyber-enabled world

Jim Hendler, professor of computer science at Rensselaer Polytechnic Institute, observed, "Automobile accidents have not kept people from driving, burglary doesn't keep people from owning houses with nice things in them and workplace violence doesn't keep people from holding jobs. Society finds ways to control these things, by a combination of social and technical means, and while none are completely removed, they are kept to a level people can tolerate – locks are put on doors, laws are passed, policemen are hired and society adjusts. The cyber-enabled world will need to create analogous mechanisms, which will happen as awareness of threat increases, and impacts will be controlled. There will be a period of adjustment (as bad things happen), followed by a demand for change, and that will motivate (through financial incentives and/or legal penalties) change."

Risk is a part of life and IoT security will improve

Robert Atkinson, president of the Information Technology and Innovation Foundation, observed, "Most adults in the U.S. drive cars even though it entails risks. Most adults will use IoT devices even though they involve risks because the benefits will vastly outweigh any potential risks. Moreover, as IoT progresses security will improve."

People will have little choice but to participate in the Internet of Things

Alice Marwick, a fellow at Data & Society, wrote, "Opting out of the Internet of Things will become increasingly difficult, as devices from automobiles to alarm clocks will be equipped with proprietary internet-enabled software. The ability of people to tinker with their own devices, choose whether they want internet connectivity and select non-connected devices will decrease, making opting out onerous, expensive and disadvantageous. This is similar to the body scanners in airports, where one can opt out, but it has a cost. Currently, data breaches are widespread, but the cost of opting out (of, for instance, credit cards) generally outweighs the risk. People will have little choice but to participate in the Internet of Things."

Opting out is not viable: How does one 'disconnect' from a home, city, airport, health care?

Kate Crawford, a well-known internet researcher studying how people engage with networked technologies, said, "This question assumes that disconnecting remains a socially and economically

viable option. For many millions of people, it simply won't be. Quite apart from the individual use of devices and platforms, the infrastructure of everyday life will be networked. How does one 'disconnect' from your home, city, airport or health care system?"

Fixes are hard to conceive, but people might not have a choice

Rebecca MacKinnon, director of New America's Ranking Digital Rights initiative, wrote, "Innovations in governance, accountability, security and industry coordination (without collusion) are going to need to advance in ways that are hard to conceive at this point in time. People with real security concerns are going to want to disconnect but the question is whether they will have a choice. In some parts of the world, perhaps not."

'The likely consequence will be more catastrophic events'

Marc Rotenberg, executive director of the Electronic Privacy Information Center, said, "The essential problem is that it will be impractical for people to disconnect. Cars and homes will become increasingly dependent on internet connectivity. The likely consequence will be more catastrophic events."

The cost and severity of lapses and breaches will be 'a constant, ongoing burden for all'

Anil Dash, entrepreneur, technologist and advocate, observed, "People will continue to connect out of necessity, but the cost and severity of lapses and breaches will increase until it's a constant, ongoing burden for all."

Newly empowered users will prevail; it is an 'Age of Amateurs'

David Brin, author of "The Transparent Society" and "Existence" and a leader at the University of California, San Diego's Arthur C. Clarke Center for Human Imagination, wrote, "Both are true [there will be more connection and some will disconnect]. We seldom note a major recent trend, an Age of Amateurs. Already we are in an era when no worthwhile skill is ever lost if it can draw the eye of some small band of amateurs. Today there are more expert flint-knappers than in the Paleolithic, more sword-makers than the Middle Ages. There is vastly more surface area of hobbyist telescopes than instruments owned by all governments and universities put together. Networks of neighbors have started setting up chemical sensors that will weave into hyper environmental webs. This will augment. For every couch or web potato, there will be two who use these new powers to become more vivid in real life."

Only choose 'libre software'-connected devices

Richard Stallman, president of the Free Software Foundation and Internet Hall of Fame member, said, "I will do my utmost to convince people to reject internet-connected devices that contain any non-libre software, by teaching people that they cannot possibly deserve our trust. See [this article] for why that is so."

The benefits of being connected 'outweigh the risks'

Jeff Jarvis, professor at the City University of New York Graduate School of Journalism, observed, "It wasn't long ago that it was said no one would ever put their credit cards online. Then came Amazon. The benefits of being connected far outweigh the risks. There are more than enough worrywarts and regulators to watch over our safety."

No 'back-to-the-land' movement is in sight

John Markoff, senior writer at The New York Times, commented, "I see no back-to-the-land movement on the horizon."

'Off-netters' will get attention but will not add up to much

Mike Roberts, Internet Hall of Fame member and first president and CEO of ICANN, responded, "It has been demonstrated time and again that individuals will trade privacy for convenience. If a new network application promises self-perceived convenience or value, such a trade is likely. Indeed, we see it going on every day. One of the broader issues is how to deal with privacy as a social construct. Much of what we regard as privacy today is an Enlightenment idea that is associated with personal freedom and other human rights. Some regard these as 'immutable,' others as fungible in pursuit of a better life. The arguments are not going to be settled soon. Cultures of dissent will persist, and much will be made of 'off-netters,' similar to the publicity gained by today's 'off-grid' culture. Probably not a big deal in the grand scheme of things."

'New jobs and social processes will emerge to protect the IoT'

Ben Shneiderman, professor of computer science at the University of Maryland, observed, "Malicious attacks by vandals, criminals and terrorists will expand, but increasingly powerful defenses will be built. Some can be centralized and top-down, but bottom-up, community-driven strategies will emerge, along with devoted public defenders (vigilantes). New jobs and social processes will emerge to protect the IoT."

‘Everything that can be connected to the web will be’

Stowe Boyd, managing director of Another Voice, wrote, “In a world in which connected driverless transportation becomes the ubiquitous and low-cost norm, few will be concerned that occasionally a hacker can take over a vehicle and crash it, especially since tens of thousands die every year in car accidents now. That example will be the instance that proves the general case. Yes, hacking will continue, and corporations and governments will fight it, but meanwhile, the overwhelming majority of human activities and finances will move online, and everything that can be connected to the web will be.”

Those who disconnect will be outliers

Fred Baker, fellow at Cisco Systems and longtime Internet Engineering Task Force leader, said, “People will become more connected; I say this because I observe that they [already] do. There are those who disconnect; they are the outliers. It would be a good thing if our public institutions sought to make ‘things’ more secure and safe, and some of those institutions do try. However, other public institutions seek to tear down the exact things that improve our security, such as by asking for 1) law enforcement access to encrypted communications, or 2) the outright technological ban of certain kinds of communications. They ask for it because 1) they are deluded into believing that only law enforcement would have access to the revealed information, which runs counter to the experience of the Los Angeles Police Department in two cases in the 1990s and of the Greek government in 2002. If there is a way to have access to that communication by anyone, even if ‘anyone’ is composed entirely of incorruptible saints, there is a way for military enemies and organized crime to have access as well. They also ask 2) because they don’t understand the capabilities, or lack of capabilities, in technology. If, for example, one would like all al-Qaida and ISIS propaganda to be magically filtered away and unavailable, ask how well we have done with pornography. We say, ‘Where there is a will, there is a way,’ and that applies both to the evil and the good.”

‘Massive work is needed’ to make the Internet of Things function

Randy Bush, research fellow at Internet Initiative Japan and Internet Hall of Fame member, commented, “People will ignore the continuous IoT disasters, and the press will minimize them. We paper over IoT security issues, yet massive work is needed here.”

‘People will just hope that the institutions around them won’t harm them’

danah boyd, founder of Data & Society, commented, “There will be no choice. As a result, many people will just hope that the institutions around them won’t harm them, while some people will feel very acute pain because they don’t fit into the system in an acceptable way.”

This is the early break-in phase; things will get better over time

Doc Searls, journalist, speaker and director of Project VRM at Harvard University's Berkman Center for Internet and Society, wrote, "The Internet of Things is a misnomer, at least as of today. What we have instead is what Phil Windley, PhD, calls a 'Compuserve of Things.' His summary: 'On the Net today we face a choice between freedom and captivity, independence and dependence. How we build the Internet of Things has far-reaching consequences for the humans who will use – or be used by – it. Will we push forward, connecting things using forests of silos that are reminiscent the online services of the 1980s, or will we learn the lessons of the internet and build a true Internet of Things?' Connectivity for things today is where connectivity for people and computers were in the 1980s and early 1990s, when the closest things we had to the internet were Compuserve, AOL, Prodigy and other 'online services' that didn't interact with each other. Likewise today we have the Google of Things, the Apple of Things and the Amazon of Things – all of them closed corporate systems. Worse, many of the connected things we are sold today spy on us, usually without our permission. Some cars report our driving to insurance companies. Some Samsung TVs watch and listen to viewers in living rooms, so Samsung can sell that data to other parties for advertising purposes. This is not only appalling on its face, but it will be flushed out by both market resistance and regulations such as the EU's General Data Protection Regulation. The only way to fully reduce vulnerability to surveillance and other forms of bad acting is to give individuals full control over the things in their lives. Today we are only beginning to evolve toward that end state; but the demand will be there, which is why there will be a business in it, and it will come to pass. Once it does, much better information will flow from people who own things to the companies that make and service those things. And spying won't be required. Between now and then we will continue to face Dr. Windley's choice."

'When it comes to the Internet of Things and data breaches, winter is coming'

Amy Webb, futurist and CEO at the Future Today Institute, wrote, "Historically, we have not seen a positive correlation between large-scale hacking attacks and significant numbers of people disconnecting from devices or services. After breaches at some of our largest retailers and entertainment providers, such as Sony and Target, consumers went right back to paying for their goods and services. When it comes to technology, if it makes our lives easier, we will continue to use it, even when risk is associated. Look no further than Uber, a service that changes its prices regularly, sometimes with increases up to five or six times above what they would be otherwise. We might complain, but the fact is that we continue using the service, even when it makes no financial sense. Technology can be like junk food. We'll consume it, even when we know it's bad for us. There is no silver bullet. The only way to effectively prevent against malware and data breaches is to stay continually vigilant. To borrow an analogy from 'Game of Thrones,' we need a Night's Watch for security. Because when it comes to the Internet of Things and data breaches, winter is coming.

Organizations must hire enough knowledgeable staff to monitor and adjust systems, and to empower them to keep pace with hackers. IT and security staff must be willing to educate themselves, to admit when they need help and to demand that executives make decisions proactively."

'Most people don't care about security or privacy until they have experienced a breach'

Brad Templeton, chair for computing at Singularity University, wrote, "Few will disconnect even if there are strong arguments for it. (Self-driving cars will be only marginally connected to their HQs due to security concerns.) When the connections are set up by security pros, they will be more minimal. When set up by the public they will be promiscuous. We need to completely replace our existing operating systems (Windows, Mac, Linux, Android, etc.) to actually make these devices safe, and we must limit their connectivity, but the convenience that comes from not doing those things will win, since most people don't care about security or privacy until they have experienced a breach."

'If such systems prove to be unreliable, people will leave in droves'

Vinton Cerf, vice president and chief internet evangelist at Google and Internet Hall of Fame member, wrote, "This will happen if devices come on the market that require online or at least local communication and programmable control. There are many risks that reliability and safety will suffer unless the makers are diligent about protecting user interests. It could be impossible to escape increased connectivity. Look at present dependence on Google Maps or generally on mobiles and apps in the last 10 years. Reliability will be key. If such systems prove to be unreliable, people will leave in droves. So that's a primary requirement. Safety is also a primary requirement. Privacy, security are part of the mix but the top two are reliability and safety."

Be less concerned with hackers and more concerned about the ways data will be used

Judith Donath of Harvard University's Berkman Klein Center for Internet & Society wrote, "People will move more deeply into connected life – and they also will be moved there whether they want to be or not. The connection of the physical world to information networks enables the collection of an unimaginably vast amount of data about each of us, making it possible to closely model how we think and to devise increasingly effective ways of influencing how we act and what we believe. Attaining this ability is extraordinarily valuable to anyone with something to sell or promote. The crucial key is getting people to provide the data, and it's not surprising that we're already seeing many once stand-alone objects (watches, heart rate monitors, thermostats, cameras, house keys and so on) turn into data-collecting network devices. My concern with the safety of things that are part of deeply connected world is not about its security and the dangers of being hacked (though those are real, and quite serious) but with the dangers that come with their intended

uses: collecting a vast amount of intimate data about each person, while weaving themselves into everyday life as a source of great convenience and pampering.

The internet will become more like a utility

David Lankes, professor and director at the University of South Carolina's School of Library and Information Science, said, "There is an interesting shift when a feature or service becomes a utility. It becomes simultaneously expected and invisible. You flip on the light switch and you simply expect power to be delivered while simultaneously becoming less aware of *how* that happens. You expect roads to take you to a destination but have little knowledge (or concern) with what the road is made of (concrete, asphalt, new materials). This leads to a series of troubling issues. Take those roads. We assume, as a utility, they are available, but don't know specifics. Specifics like bridges aging out of service. We only become aware of the importance of both availability and service assurance when something goes wrong. Even then, we still drive on the next bridge assuming that the failed one was an anomaly, or that a failed bridge will spur action. The Internet of Things is nothing more or less than the evolution of the internet to a utility. We don't think about our refrigerators having IP addresses, or our cars linking to Wi-Fi because we simply assume they will. The value we get is too high not to take the risk – particularly because the risk is hidden or minimized."

Security must improve, but 'need will drive manufacturers to provide secure solutions'

Galen Hunt, partner research manager at Microsoft Research NExT, urged, "The security of IoT must improve. As more devices attach, consumers and enterprises will grow in their understanding of the profound need for secure systems; this need will drive manufacturers to provide secure solutions."

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 one of eight questions asked by Pew Research Center and Elon University's Imagining the Internet Center in an online canvassing conducted between July 1 and August 12, 2016. This is the seventh "Future of the Internet" study the two organizations have conducted together. For this project, we invited nearly 8,000 experts and members of the interested public to share their opinions on the likely future of the internet, and 1,537 responded to at least one of the questions we asked. This particular report covers responses to one of five questions in the canvassing. Overall, 1,201 people responded and answered this question:

> ***As billions more everyday objects are connected in the Internet of Things, they are sending and receiving data that enhances local, national and global systems as well as individuals' lives. But such connectedness also creates exploitable vulnerabilities. As automobiles, medical devices, smart TVs, manufacturing equipment and other tools and infrastructure are networked, is it likely that attacks, hacks or ransomware concerns in the next decade will cause significant numbers of people to decide to disconnect, or will the trend toward greater connectivity of objects and people continue unabated?***
>
> *The answer options were:*
>
> *Significant numbers will disconnect - 15%*
>
> *Most people will move more deeply into connected life - 85%*

Then we asked: *Please also consider addressing these issues in your response. You do not have to consider any of these. We have added them because we hope they might prompt your thinking on important related issues: What is the most likely kind of physical or human damage that will occur when things are networked? How might governments and technologists respond to make things more secure and safe? Is it possible to network physical objects in such a way that they will generally remain safe for the vast majority most of the time?*

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 six "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 global internet governance 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 and policy people from technology businesses; government, including the National Science Foundation, Federal Communications Commission and European Union; 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; technologists and innovators; top universities' engineering/computer science departments, business/entrepreneurship faculty, 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 80% 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," 25% identified themselves as research scientists; 7% as entrepreneurs or business leaders; 8% as authors, editors or journalists; 14% as technology developers or administrators; 10% as advocates or activist users; 9% as futurists or consultants; 2% as legislators, politicians or lawyers; and 2% as pioneers or originators. An additional 25% 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:

Robert Atkinson, president of the Information Technology and Innovation Foundation; **Fred Baker**, fellow at Cisco; **Naomi Baron**, a professor of linguistics at American University; **danah boyd**, founder of Data & Society; **Stowe Boyd**, managing director of Another Voice; **Marcel**

Bullinga, trend watcher and keynote speaker; **Randy Bush**, Internet Hall of Fame member and research fellow at Internet Initiative Japan; **Jamais Cascio**, distinguished fellow at the Institute for the Future; **Barry Chudakov**, founder and principal at Sertain Research and StreamFuzion Corp.; **David Clark**, Internet Hall of Fame member and senior research scientist at MIT; **Cindy Cohn**, executive director at EFF; **Anil Dash**, entrepreneur, technologist and advocate; **Cathy Davidson**, founding director of the Futures Initiative at the Graduate Center of the City University of New York; **Cory Doctorow**, writer, computer science activist-in-residence at MIT Media Lab and co-owner of Boing Boing; **Judith Donath**, Harvard University's Berkman Klein Center for Internet & Society; **Stephen Downes**, researcher at the National Research Council of Canada; **Bob Frankston,** internet pioneer and software innovator; **Oscar Gandy**, professor emeritus of communication at the University of Pennsylvania; **Marina Gorbis**, executive director at the Institute for the Future; **Jeff Jarvis**, a professor at the City University of New York Graduate School of Journalism; **Jon Lebkowsky**, CEO of Polycot Associates; **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; **Rebecca MacKinnon**, director of Ranking Digital Rights at New America; **John Markoff**, author of "Machines of Loving Grace: The Quest for Common Ground Between Humans and Robots" and senior writer at The New York Times; **Jerry Michalski**, founder at REX; **Andrew Nachison**, founder at We Media; **Frank Pasquale**, author of "The Black Box Society: The Secret Algorithms That Control Money and Information" and professor of law at the University of Maryland; **Demian Perry**, director of mobile at National Public Radio; **Justin Reich**, executive director at the MIT Teaching Systems Lab; **Mike Roberts**, Internet Hall of Fame member and first president and CEO of ICANN; **Michael Rogers**, author and futurist at Practical Futurist; **Marc Rotenberg**, executive director of EPIC; **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; **Doc Searls**, journalist, speaker and director of Project VRM at Harvard University's Berkman Klein Center for Internet & Society; **Ben Shneiderman**, professor of computer science at the University of Maryland; **Richard Stallman**, Internet Hall of Fame member and president of the Free Software Foundation; **Brad Templeton**, chair for computing at Singularity University; **Baratunde Thurston**, a director's fellow at MIT Media Lab, Fast Company columnist and former digital director of The Onion; **Patrick Tucker**, technology editor at Defense One and author of "The Naked Future"; **Steven Waldman**, founder and CEO of LifePosts; **Jim Warren**, longtime technology entrepreneur and activist; **Amy Webb**, futurist and CEO at the Future Today Institute; and **David Weinberger**, senior researcher at Harvard University's Berkman Klein Center for Internet & Society.

Here is a selection of some of the institutions at which respondents work or have affiliations:

AAI Foresight, Access Now, Adobe, Altimeter Group, The Aspen Institute, AT&T, Booz Allen Hamilton, California Institute of Technology, Carnegie Mellon University, Center for Digital Education, Center for Policy on Emerging Technologies, Cisco, Computerworld, Craigslist, Cyber Conflict Studies Association, Cyborgology, Dare Disrupt, Data & Society, Digital Economy Research Center, Digital Rights Watch, DotTBA, EFF, EPIC, Ethics Research Group, European Digital Rights, Farpoint Group, Federal Communications Commission, Flipboard, Free Software Foundation, Future of Humanity Institute, Future of Privacy Forum, FutureWei, Gartner, Genentech, George Washington University, Georgia Tech, Gigaom, Gilder Publishing, Google, Groupon, Hack the Hood, Harvard University's Berkman Klein Center for Internet & Society, Hewlett Packard Enterprise, Human Rights Watch, IBM, InformationWeek, Innovation Watch, Institute for Ethics and Emerging Technologies, Institute for the Future, Institute of the Information Society, Intelligent Community Forum, International Association of Privacy Professionals, ICANN, Internet Education Foundation, Internet Engineering Task Force, Internet Initiative Japan, Internet Society, NASA's Jet Propulsion Laboratory, Karlsruhe Institute of Technology, Kenya ICT Action Network, KMP Global, The Linux Foundation, Lockheed Martin, Logic Technology Inc., MediaPost, Michigan State University, Microsoft, MIT, Mozilla, NASA, National Institute of Standards and Technology, National Public Radio, National Science Foundation, Neustar, New America, New Jersey Institute of Technology, The New York Times, Nokia, Nonprofit Technology Enterprise Network, New York University, OpenMedia, Oxford Martin School, Philosophy Talk, Privacy International, Queensland University of Technology, Raytheon BBN Technologies, Red Hat, Rensselaer Polytechnic Institute, Rice University's Humanities Research Center, Rochester Institute of Technology, Rose-Hulman Institute of Technology, Semantic Studios, Singularity University, Social Media Research Foundation, Spacetel, Square, Stanford University's Digital Civil Society Lab, Syracuse University, Tech Networks of Boston, Telecommunities Canada, Tesla Motors, Department of Defense, US Ignite, UK Government Digital Service, Unisys, United Steelworkers, University of California (Berkeley, Irvine, Los Angeles and Santa Barbara campuses), University of Copenhagen, University of Michigan, University of Milan, University of Pennsylvania, University of Toronto, Vodafone, We Media, Wired, Worcester Polytechnic Institute, Yale University, York University.

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

http://www.elon.edu/e-web/imagining/surveys/2016_survey/internet_of_things_infrastructure.xhtml
http://www.elon.edu/e-web/imagining/surveys/2016_survey/internet_of_things_infrastructure_credit.xhtml
http://www.elon.edu/e-web/imagining/surveys/2016_survey/internet_of_things_infrastructure_anon.xhtml

Theme 1: People crave connection and convenience, and a tech-linked world serves both goals well

A lot is at stake as the Internet of Things rolls out, and many of its creators are betting that people will wear connected devices, appreciate smart appliances, drive in connected cars, thrive in smart cities, understand vastly more about a sensor-saturated world and build businesses around analytics-assisted supply chains.

There is no one official method for measuring the growth and size of the IoT at this point, and projections tend to vary widely. Here are several estimates:

- IHS Economics forecasts that the IoT market will grow to an installed base of 75.4 billion connections by 2025. Huawei estimates it will have 100 billion connections by 2025.
- Gartner analysts estimate that total spending on IoT endpoints and services will reach nearly $2 trillion in 2017.
- Juniper predicts that the number of connected devices, sensors and actuators will exceed 46 billion by 2021.
- Forrester reports that transportation applications – including tracking and services in cars, trucks, trains, ships and more – are the most rapidly expanding category of internet-connected things, as are security and surveillance applications in business and government, management of supply chains, inventory, facilities, industrial assets and energy, and "smart" consumer products – smart TVs, smart LED lighting, HVAC, video and security systems.
- Boston Consulting estimates that by 2020 $267 billion will be spent on IoT technologies, products and services. Among the chief use cases for this spending are predictive maintenance, self-optimizing production, automated inventory management, remote patient monitoring, smart meters, track and trace, connected cards, distributed generation and storage, fleet management and demand response.
- Bain projects that by 2020 annual revenues for IoT hardware, software and logistics businesses could exceed $470 billion.
- IDC forecasts that by this year 60% of global manufacturers will use analytics to sense and analyze data from connected products and manufacturing, and by 2018 the proliferation of advanced, purpose-built analytic applications aligned via the IoT will result in 15% productivity improvements.
- General Electric estimates the Industrial Internet of Things (IIoT) has potential to generate revenues of up to $11.1 trillion on an annual basis by 2025 – 70% of which would come via business-to-business solutions. GE predicts that investment in the IIoT will top $60 trillion in the next 15 years. Even industrial robots such as those used on vehicle assembly lines – there are more than 1 million today and 2.5 million are expected to be in use by 2019 – are networked.

- Cisco says connected-home, machine-to-machine connections will reach 5.8 billion in 2020, and there will be a tripling of online traffic by then due to the addition of 10 billion new devices and connections in the next several years. Cisco and Arbor Networks also report that security concerns are on the rise, projecting that the number of attacks online will triple in the next five years.
- IoT security is on everyone's mind, and organizations like the Internet Society (ISOC) and the Internet Engineering Task Force are discussing best practices. ISOC urges more attention be paid by all involved in developing the IoT to serve the public good, noting that the scope, complexity and changing nature of this system increases challenges in security, surveillance, tracking, data rights and other concerns and requires immediate attention in regard to reacting responsibly to potential regulatory, legal and rights issues.

A majority of these respondents wrote about the double-edged reality that the IoT will create. They note that vulnerabilities will proliferate, but point out that connectivity and convenience have their own momentum and logic. They predict that for most people in most cases the risks will be seen as small when weighed against the benefits of connectivity and convenience.

It's only human to connect, and there are many advantages. It's magical, even addictive

Shawn Otto, organizational executive, speaker and writer with ScienceDebate.org, brought up the point that the brain-computer interface may soon network people's minds online. He wrote, "The conveniences will outweigh the risks for many people, and the affordability of the Internet of Things will in many cases slant the playing field in the consumer's favor. The stakes will be higher for more expensive personal things such as cars, homes, bank accounts, computer systems and the cloud, or things that carry emotional meaning, such as access to cloud-stored personal musical or photographic collections, and together these higher-stakes items will be the greater focus of criminal activity. Additionally, as the computer/brain interface becomes increasingly robust and our knowledge about commandeering certain brain centers – including perception and motivation – grows, *human hacking* may become less a matter of science fiction and more a serious psychological, legal and law-enforcement concern. In general, the emerging questions of human agency and free will are just over the next hill."

An **anonymous IT director at a technology network** said, "I'm sure there will be plenty of instances where an IoT hack has terrible consequences for someone. However, this is also true for our current online systems and activities, but despite all those cases we continue to see people moving more deeply into connected life rather than disconnecting. The heart of it is that the benefits of connected life (for most people) far outweigh any potential risks, and I expect that to remain true as the IoT expands to every corner of our society."

Micah Altman, director of research at MIT Libraries, observed, "The network of IoT is at an earlier stage than that of social networks – and there is less immediate value returned, and not yet a dominant network of these devices. It may take some time for a valuable network to emerge, and so the incentives to use IoT seem, so far, small for the end-consumer while the security issues loom large given the current lack of attention to systematic security engineering in design and implementation of these systems. (The lack of visibility of security reduces the incentives for such design.) However, it seems likely that within the next decade the value of connected devices will become sufficient to drive people to use, regardless of the security risks, which may remain serious, but are often less immediately visible."

Valerie Bock of VCB Consulting said, "No human advances come without unexpected negative consequences. We will likely continue to see dramatic and upsetting negative consequences, both unintended and as the result of malfeasance from growing interconnectivity. But the advantages of connectivity really do seem to come close to the square of the number of people connected. Whether it also will square with the number of things connected remains to be seen – I expect that the value of connecting things will not be as dramatic as the value of connecting people, and that we will learn how to make these connections sufficiently secure that people will continue to choose to make them."

Hume Winzar, associate professor in business at Macquarie University in Australia, said, "Disconnecting from the network would mean disconnecting from much of society. No hospital care, no TV, no news services, no telephone. Some will attempt it but most will not. The majority (90%?) of connected devices will produce data that are worthless except for the subsystem gathering the data. The other 10% will be aggregated data/information that are invaluable."

An **anonymous assistant director** wrote, "I'm always concerned about alarmists who think that every new technology will be the end of humanity (just read about how people felt about the printing press when it was invented). Sure there are dangers of allowing physical objects to be network-connected, but this ability also allows them to be updated and patched to prevent exploits. The benefits of smart devices can be huge. In my latest Nest Thermostat report it states, 'Since 2011, Nesters have saved 7,681,837,833 kWh.' I also read a report that utilities can use smart thermostats (with owners' permission) to make slight changes to the timing and temp (5-minute delay and half a degree for example – unnoticeable by the homeowner) to eliminate the need for bringing reserve power online during peak usage. Basically they can use this network of thermostats as a reserve power plant. Examples like these in my opinion will reach every aspect of life, making us more efficient and able to use our things more intelligently. Once people start seeing the time and cost advantages of connecting their things the security and other issues will be worked out."

Stephan G. Humer, head of the internet sociology department at Hochschule Fresenius, a private university in Berlin, commented, "We've just seen the early stages of digitization, so there is only one direction: More and more people will move deeply into connected life."

Bernardo A. Huberman, senior fellow and director of the Mechanisms and Design Lab at HPE Labs, Hewlett Packard Enterprise, observed, "Networked things can lead to large, extended damage to a system. But we have not witnessed such a breakdown yet, and so people perceive the advantages of being connected and provided with services that were unheard of years ago. Uber and Lyft are great examples of what IoT can do for us. As time goes on, many more services based on the existence of networked smart sensors will appear."

James McCarthy, a manager, wrote, "There's always a downside to an upside, and an upside to a downside – and in the case of internet access, the upside is enormous. The advantages and benefits offered by access to the internet are far more attractive than the various risks and downsides. And – to refer to your example of automobiles – the options that don't use some sort of connection are decreasing in number, particularly with the recent initiatives to move to autonomous vehicles. Frankly, I'm okay with this."

David Durant, a business analyst in the UK Government Digital Service, replied, "Digital channels are increasingly seen as the only sensible way to interact with friends, work, business and the state. This will continue as more IoT items become available. Driverless cars or household 'robots' (e.g., Amazon's Alexa) will be seen as something safe and entirely normal to use."

Matt Hamblen, senior editor at Computerworld, responded, "Nearly everybody will connect to devices without hardly a worry about privacy or loss of personal data. There will just be too many advantages to being connected with a smartphone or smart wearable devices. Cars will imperil passengers if they are autonomous, but people will put up with the risk, eventually. People looking at cellphones while walking will still walk into traffic, but perhaps the devices they use will be able to warn them as they move about."

Ben Railton, professor of English and American studies at Fitchburg State University, said, "I'm sure some folks will disconnect, and I hope that opportunity remains and will always remain a viable one. But, for the vast majority, increasing connection is both inevitable and an integral part of how we live and operate in society."

Some said the craving for connectivity and convenience combines with one more element to make it impossible for some not to stay on board with the IoT: the drive within some to adopt the newest, magical tech toys. An **anonymous respondent** observed, "Innovators are putting more into what

they [these tools] can do rather than how to keep them safe. People are influenced by gee-whiz gizmos, frequently at the expense of safety."

An **anonymous lead field technician** said, "People as a rule are lazy and fascinated with gadgets. Almost no lay people have even the most rudimentary knowledge of how computer/network security works, and manufacturers of 'smart' devices design products lacking in or ignorant of that knowledge."

Mike Warot, a machinist at Allied Gear, wrote, "People deeply discount the future costs of flaws in things they buy today. The big shiny new toy will always get bought."

An **anonymous data center technician** replied, "Currently, marketing is stronger than people."

As life increases in complexity, convenience is the default setting for most people

Many of those who are positive about the IoT's future argued that a major driver of IoT adoption will be people's desire for convenience and for goods and services facilitating a low-friction life in an environment of accelerating complexity, information overload and the apparent shrinkage of time. Most participants in this canvassing say people will not withdraw from IoT systems because they will make life easier and better.

Scott McLeod, associate professor of educational leadership at University of Colorado, Denver, said, "There will be all kinds of hiccups, horror stories, accidents, deliberate acts of sabotage and other bumps along the road that will slow but not stop our greater connectivity. Convenience and empowerment always seem to win for most people, even at some loss of privacy, control or transparency."

Charlie Firestone, communications and society program executive director and vice president at The Aspen Institute, observed, "The lure of convenience will continue to attract people. Those who disconnect will mostly be people who were actually personally affected."

An **anonymous IT manager and systems administrator** said, "The concerns around the Internet of Things and hacking/privacy are completely legitimate, but this will not stop or even significantly slow the march of progress. Identity theft hasn't stopped millions from using online banking. Phishing and ransomware haven't stopped millions or even billions from using email. It's true that someone hacking into your medical device or your car is scarier than hacking into your email, but ultimately convenience trumps security. People will give up a measure of security if it

makes their life easier. The security experts behind the Internet of Things will just have to make sure that their security measures are strong enough that the convenience outweighs the risk."

An **anonymous director of evaluation and research** said, "Except for maybe supersonic transport, we really haven't seen a situation where people eschew convenience – unless they're convinced of direct threats to their health. Making it all safe will be one of the main industries of the future. We'll take the cyber-muggings (and worse) with the new world – just in the way we've always taken the new dangers (auto crashes, chemical poisonings) as a natural part of the inevitable march of progress."

Paul Davis, a director based in Australia, said, "As digital devices and connectivity become ubiquitous, being 'connected' will become simpler than not. The benefits of the connected life, particular in the area of health and lifestyle outcomes, will outweigh risks of privacy loss. However, the challenge of a post-growth world where automation and algorithms have replaced most of the need for labour will present significant societal challenges."

Sam Anderson, coordinator of instructional design at the University of Massachusetts, Amherst, said, "The benefits will be too appealing (and likely too immediately societally beneficial) to turn away from. There will be some communities that turn away, but they will be a minority. It may be that many people try to partition their lives into connected (most of the time) and unconnected (for quiet, for deep work)."

Ian Peter, an internet pioneer and historian based in Australia, said, "I expect people to put convenience over risks and expand their usage of connected devices. They may feel trapped and disillusioned, but that won't necessarily lead to them ceasing usage."

An **anonymous political science professor** replied, "The lure of comfort and convenience can only be countered by extremely huge disasters, apparently. Multiple firms and governments losing – or just giving away – the private data of millions isn't huge enough."

Dave Howell, a senior program manager in the telecommunications industry, wrote, "Convenience. Autonomous automobiles are probably more than one but under two decades out (they need infrastructure), but we'll move deeper into a converged world because it's a more convenient place. Dropouts will be clustered in retirement communities or luddite compounds, mocked by the mainstream."

Aaron Chia Yuan Hung, an assistant professor at Adelphi University, replied, "There is no doubt that hackers will take advantage of the Internet of Things and pull down massive infrastructures. But

this will not deter most people from the convenience it offers. Some people will disconnect but they are likely going to be the minority."

An **anonymous network CEO** wrote, "Even as risks may increase, so long as technology is offering an easier/faster/less-expensive option people on the whole will choose it."

An **anonymous writer** explained how time-saving aspects of networked devices attract people. "While there are certainly concerns with security, people desire ease and convenience overall," he responded. "The ability to 'program' your house to have a hot meal ready just as your self-driving car delivers you from the office is quite seductive, especially as the ease of movement and increasing access to the world around you encourages people to spend more time hustling and bustling."

Additional **anonymous respondents** wrote the following, tied to people's craving for the need for connection and convenience:

- "Get on the bus or be left behind."
- "People are deluded into thinking participation equates with influence."
- "Lack of safety will not deter most people from jumping onboard with overuse (as with overuse of plastics and of antibiotics and of food preservation technologies and small electronics) if it is marketed as convenient and safe (even if it is neither)."
- "It is becoming so much easier and easier to rely completely on technology in a variety of ways that it's unlikely that people will be able to disconnect."
- "We're more likely to be victimized. It will seem so easy, until something bad happens to us."

The always-online younger generation can't imagine being anything but connected

A number of respondents said they expect that those born of the digital generation will be likely to fully embrace becoming more fully connected and, as this new breed begins to outnumber the pre-digital generation, there will be fewer folks who are suspicious of the flaws of the IoT and the foibles of those who build and maintain its many aspects.

Sam Punnett, research officer at TableRock Media, commented, "We are raising generations of people for whom the connected life is the norm."

Dana Klisanin, founder and CEO of Evolutionary Guidance Media R&D, commented, "Significant numbers of people will disconnect due to privacy concerns, however on the whole the newer generation will increasingly purchase networked 'things' as long as they can clearly see a benefit (in that item vs. the unconnected item)."

An **anonymous marketing specialist** replied, “People, not cynically but as an observation, are pretty hubristic. Connected is status quo. People don’t like to be seen as being left out of the awesomeness of stuff. They’ll just do as their friends do for the most part.”

An **anonymous respondent** replied, “The basic paradigm of the younger generations is to connect. There will always be those for whom that connection does not work, but such people will be left further and further behind. This will create other problems!”

In a related set of thoughts among the responses, some participants in this canvassing predicted that a share of older tech users might walk away from technology as the IoT expands and they elect to take life at a slower pace. An **anonymous information systems security manager** said, “A fair number may choose to disconnect. The [Baby] Boomers are retiring, and for many it may offer an opportunity to simply disengage from the online pace they have kept up.”

An **anonymous principal scientist at a large software company** replied, “It’s only us old fogies (I’m currently 73) who will back away from being connected 24/7. I, for one, don’t trust automation and I’m not on social networks. That’s in spite of (or because of) the fact that I have a PhD in computer science.”

An **anonymous communications librarian** said younger people will step up to lead in finding solutions to many IoT issues, writing, “As the Millennial generation continues to take over employment and politics in this country, more attention will be paid to these very relevant concerns.”

Theme 2: Unplugging isn't easy now, and by 2026 it will be even tougher

Another significant group of these experts made the case that people will adopt products and services tied to the Internet of Things because it is their best life choice and at times their only choice. They believe that opting out will not be an option in many situations, for example, in daily work and health care settings. A share of these respondents noted that as businesses, governments and other organizations begin to reap benefits from the IoT, people will be rewarded for their use and suffer consequences for nonparticipation. Even if there were no such carrot-stick motivations, network effects would leave the unconnected at a disadvantage. An **anonymous respondent** commented, "Disconnection and remaining in society are mutually incompatible."

Resistance is futile: Businesses will penalize those who disconnect; social processes reward those who connect. Fully withdrawing is extremely difficult, maybe impossible

Some respondents said IoT businesses will make it increasingly difficult if not impossible for people to be able to opt out of the IoT-based services, platforms and knowledge-sharing resources and still have access to resources they desire or require. The drive to continuously increase the user base by making it "sticky" and buying out or crushing competitors who might offer more choices is a standard characteristic of today's most successful digital business platforms.

Mary K. Pratt, a freelance technology journalist, commented, "Even if individuals are concerned about the risks, they'll find it difficult or impossible to opt out of these connections if they want to continue with the products or services they want and/or need."

Various anonymous respondents made these related remarks:

- "If there is money to be made, industry will push it, regardless of the inherent risks."
- "It is not really up to the people."
- "More people will just click the box, opting for convenience over security and privacy."
- "New devices will be IoT by definition so it will be hard to get 'offline.' "

Eugene H. Spafford, a professor at Purdue University and an expert in computer security issues, wrote, "It appears that vendors do not appreciate the dangers involved in IoT, and offerings that don't incorporate connectivity are increasingly rare. … IoT is being pushed as the norm, and the majority of people do not seem to be aware of the hazards, so they are thus driving the market in that direction."

An **anonymous senior software engineer at Microsoft** wrote, "Societal norms will dictate to connect. Products will dictate to connect. Entertainment needs will require connection."

An **anonymous respondent** observed, "There will be no option but to do so as companies can extract subscription fees for use of connected devices. More items will require connectivity and hence more sharing of personal data by users. Companies are monetizing more thanks to the Internet of Things."

An **anonymous respondent** wrote, "I don't feel you will be able to disconnect. More systems will come online that require you to opt in to connectivity to achieve service. Example: Progressive Insurance's Snapshot dongle to record your car's performance and data-mine for driving behaviors and accidents. Currently this program is voluntary, but how easy would it be to require all drivers to be monitored for coverage? This will become the norm and will proliferate throughout our daily life."

Another **anonymous respondent** said, "The question is posed as if there is meaningful choice. There is not. Are you really going to opt out of that implanted heart device out of concerns for malware? I don't remember where technologies that increase surveillance and decrease the value of labor have failed in the marketplace. That's not end-user demand, that's the inhumanity of capitalism."

Antero Garcia, assistant professor at Colorado State University, wrote, "The grip of capitalist ecosystems – Apple, Google, Facebook, etc. – is strengthening the ability to connect multiple aspects of our lives online. It will be harder to disentangle from this system moving forward."

Respondents in this study generally say it is already difficult and it will become increasingly more difficult to find unconnected platforms, services and products and avoid participating in a connected world. These experts argue that unplugging invites loneliness and a substandard life. Most believe it is not a realistic option for most people. **Dave McAllister**, director at Philosophy Talk, said, "Those who disconnect will end up as a class with diminishing resources. Information is king, and connectivity will power that."

Christopher Owens, an adjunct professor at Columbus State Community College in Ohio, said, "Being connected is becoming less and less of a choice, so even if someone wanted to disconnect, they would not realistically be able to, any more than people 20 years ago could stop driving, using the telephone or having a bank account. Too much of modern life is dependent on having near-constant internet access."

An anonymous **associate professor at a state university** wrote, "Most people will move more deeply into connected life because they will face significant penalties to social capital, accessibility of goods and services, and work opportunities if they do not. … The vulnerabilities created by interconnected devices are very real, and will disproportionately impact the most marginalized."

An **anonymous respondent** wrote, "The fear of missing out will win out over concerns of potential security threats. Systems will reinforce this, compelling people to maintain digital connection. Kind of like how often Social Security numbers are required to get a thing done. It's not secure, and they shouldn't be required, but it has become requisite to use them in order to access many services."

Ryan Hayes, owner of Fit to Tweet, commented, "The divide in capabilities between the most-connected and the least will define who gets the valuable jobs. Technology should be making life better too, not just more productive, so disconnecting will be opting out from those benefits; it will sabotage their abilities to get more out of life, like someone deciding not to learn how to read because they're afraid they'll read something dangerous to them."

David Banks, co-editor of Cyborgology, said, "Disconnection from networks of capital and information generally come at a high price for individuals and even entire communities. As more parts of our lives become connected to the IoT it seems likely that disconnection will become a privilege to those that can afford to, for example, forgo the savings on car insurance that come with agreeing to be tracked."

An **anonymous chief marketing officer** replied, "Breaches and security concerns may likely grow and they may create sensational headlines and a high-profile disconnectors movement, but the proliferation of connected and networked devices will become so critical to our lives that those who choose to disconnect will be considered the fringe, akin to those who shunned electricity and automobiles in the 20th century."

Joe Mandese, editor-in-chief of MediaPost, said, "People will become more dependent on technology for accessing data and connecting with other people and other things, despite nefarious practices by hackers."

An **anonymous professor** observed, "Technological advances are simply making life's most boring aspects more efficient and easier to complete. At the same time, people's jobs demand increasingly more time and effort. As a result, the efficiencies produced by technology (say in banking or home security or shopping) become necessary instead of remaining as luxuries. No one can *not* use online services any more. At the same time (and not unrelated to the increased

requirement for work hours), businesses are reducing the number of people who work for them and who are able to assist customers in person. As a result, whether people are skeptical or not, they will be forced to conduct their business online and to include other connected services in their daily lives."

An **anonymous respondent** commented, "Disconnecting will take time and energy. Most will not [make the effort to disengage]. The outliers and anarchists will revel in it."

An **anonymous professor of digital media at an Australian university** said, "The choice to disconnect will be a hipster privilege. Most people's lives will become increasingly entangled with internet connectivity, although much of the seamless interoperability and user benefit will be glitchy, full of security errors and underused by consumers."

Will Kent, an e-resources librarian at Loyola University-Chicago, replied, "People won't have the choice to disconnect. Take applying for jobs as an example. It is nearly impossible to apply for a job without a computer or email. Soon it will be that way for housing and for all communication and appliances."

David Krieger, director of the Institute for Communication & Leadership, based in Switzerland, commented, "There is no opt-out for the internet. No one can disconnect. Algorithmic automation will create overly complex systems of communication, transportation, energy, finances, production, etc., that are no longer under control of anyone."

An **anonymous assistant professor at a public research university** said, "People will dive more deeply because they will have to. Institutions will effectively offer no viable alternative to cloudware systems for medical treatment and information access."

Dmitry Strakovsky, a professor of art at the University of Kentucky, said, "Most people are *waaaay* too comfortable with easy-to-use mobile systems to forgo the experience of the connected world. Security will be an increasing concern but it will not deter any serious number of consumers. We will simply move deeper into biometrics land. The bigger issue is going to be further down the line when we finally have access to quantum computing and no encryption will be enough. Then we are in trouble."

Jon Hudson, futurist and principal engineer, wrote, "The sad thing is, you won't have a choice. Disconnecting will not only hurt you and your earning capabilities, but also those of your children and anyone else living in your house. We all must get more and more connected if we want to see where this is going and reach that next level. Whatever it is."

John Bell, software developer, data artist and teacher at Dartmouth College, wrote, "More people will become more connected, but largely because individuals won't have any choice but to participate in connected technologies due to market forces that encourage centralization and constant connection. This will continue until there is a global security event that causes governments to intervene, like a war where infrastructure technology is targeted. Technologists could solve this problem by, for example, using completely different networking protocols for IoT devices than are used on the commercial internet. Another possibility would be engineering home-automation servers that only operate locally. However, there is not enough awareness of or concern about the potential security problems of always-on cloud services to force companies to develop local solutions when there are vast economic benefits for those companies to make sure devices must be connected to their services."

Mary Griffiths, associate professor in media at the University of Adelaide, South Australia, wrote, "Smart cities are already developing across the world with responsive street lighting, traffic lights, and immersive civic spaces. The benefits can include better air monitoring; smoother traffic flows; faster ambulance and police response times; and municipal planning more finely attuned to a population's needs. Those who are not 'connected' may be excluded from full participation in such cities. If they don't provide the information the city functions on, their needs can't be part of planning based on predictive trends."

Some respondents clearly noted that while most people will continue to become more connected in the future, they will – at least at times – strongly resent it. An **anonymous user experience manager** observed, "We'll probably be pulled in, like it or not. One won't be able to buy anything other than the proverbial internet-ready toaster, for example. Connectivity will be standard, not an upgrade, like it or not. I don't think this will happen easily, though. There will be tons of stuff that falls off the hype curve, and consumers will be angry about being forced into the new paradigm in some cases."

An **anonymous engineer at a major U.S. government technology agency** wrote, "People will move to a more connected life because they will not be allowed any other choice. It takes a fairly deep education and strength of will to constantly check each new item or service for loopholes and pitfalls. It also will get easier for bad actors to hack even those with good security. Driverless cars will be hacked (btdt – been there, done that), tea kettles will leave your network vulnerable (btdt), governments will keep knowledge of zero-day exploits to themselves and let the citizens suffer (*btdt*), and we will mostly sleep through it all. If we could stop feeling everything needs to be connected all the time, we'd have a chance. It's unlikely without a drastic change though."

An **anonymous professor of media production and theory** observed, "Disconnection is less and less of an option. In general, participation in the internet, whether of things or cerebra, offers so much we'll continue to do it, even though it also has complex and poorly understood effects on our physiologies, social relations, emotional development, etc. This is a vast new field of research not well-studied."

Frank Elavsky, data and policy analyst at Acumen LLC, commented, "The greatest security threats to those who participate in systems of connectivity have never outweighed the potential benefits of that connectivity. Of course, hacking will be a greater threat. But I believe that the threat will be so nominal that only those too fearful to continue in the connectivity will be the real victims of the system."

Vance S. Martin, instructional designer at Parkland College, observed, "If you build it, they will buy it. I am supposed to take my blood pressure every morning and email results to my doctor every few months. Wouldn't it be easier to take my blood pressure and have it automatically sent to him? That would save me 10 minutes a month. Don't we want a TV or device we can tell to find and play 'Die Hard,' or to load 'Fallout 4'? Isn't it great to have a button on your washer that you can just push to fill an Amazon order for soap? If all of these things had appeared at once, we might be put off. But with slow release and the allure of the newest, time-saving device, and the fact they become cheaper and cheaper, we will have them in our homes. If you want a refrigerator that doesn't take a picture, inventory the contents and order refills, you'll have to start buying old appliances and refurbishing them, which some will do. But who is going to remember to safeguard your blood pressure monitor or the Tide button that is hooked up to Amazon? Your cellphone, your computer, your TV may be kept secure, but not the rest. And with that will come back doors for hackers to shut down your furnace, get your account information and hold your digital photo albums hostage. This will not cause us to disconnect; it would be too difficult. It will lead to a reactive stance rather than a proactive stance for most American and global consumers."

You can't avoid using something you can't discern. So much of the Internet of Things operates out of sight that people will not be able to unplug completely

In addition, some respondents pointed out that people are already unknowingly participating in beneficial yet vulnerable interconnected systems, many of which are embedded in processes and services in which they are not clearly visible. Unless one goes completely off the grid and remains pretty much rooted in a remote area, not visible by satellite or drone, living by one's own means, a full disconnection is highly unlikely.

An **anonymous vice president of global engagement** replied, “Much of the deeper dive into connected life will be unconscious, as people forget that internet connectivity is what enables many of the conveniences they rely on. Like electricity, connectivity will be taken for granted.” And an **anonymous respondent** observed, “Really what you will have is not disconnection but anthropic connection as disconnection, or ignorance of their connection.”

Barry Chudakov, founder and principal at Sertain Research and StreamFuzion Corp., wrote, “We [have] hidden connecting IoT processes to make them more efficient, we now have to … shine light on that process stream in order to create awareness of what we have done and understand the implications of all that connectivity. … The more things we build with embodied (hidden) intelligence, the more we are challenged to match or understand that intelligence – or perhaps outwit it – if we have a different outcome in mind. If your smart car wants to drive you to the hardware store and you want to go visit your sister, there’s a clash of intentions. The obvious answer to that is the ability to override the object’s intentions. But what if you can’t? Or don’t know how? Or what if you don’t even realize the intention until you see the effects of the intention? For example, [what if] you don’t know that the algorithm programmed to stop steep market decline could, in fact, precipitate a further decline?”

Louisa Heinrich, founder at Superhuman Limited, replied, “People will certainly move more deeply into connected life, and not necessarily by choice. Cities are embedding technology, as are manufacturers of consumer goods. We will be surrounded by technology more or less all the time, and it will certainly shape our experience of the world, but we may not be able to interact with the technology on any meaningful level because it isn’t owned by us.”

An **anonymous open source technologist** commented, “I don’t think that the decision can be made to disconnect. Modern cars are already software-driven whether you like that or not. Same is true for planes. That this becomes the case for everything else is certain, and what is less certain [is] if anyone can opt out or even understand the extent of connectedness in this generation of electronics or the next.”

Lauren Wagner, a participant who shared no additional identifying details, said, “When the default is for a manufacturer to produce a connected device, consumers may not even realize what their products are connected to and how this makes them vulnerable to security breaches. When things are networked, I am most concerned about connected devices failing in real time – like self-driving cars and connected medical devices – where the cost is human life.”

An **anonymous senior software developer** wrote, “A significant number of exploits have not stopped people up until now, so why should it in the next 10 years? It is true; there will be problems.

We will have a mass car-hack incident where thousands of cars will be hacked simultaneously and caused to crash. But in the end it will not stop progress. Companies will just be forced to take security more seriously."

An **anonymous respondent** replied, "The fact is that we remain as ignorant as ever about basic security, granting 'Pokemon Go' full access to your entire Google account, or believing that posting on Facebook 'I do not give permission to Facebook' is somehow an efficacious legal strategy. I don't see people learning from anything soon. The advantages and integral part the internet plays in our lives – especially for those who grew up with it – will outweigh the fears and risks."

Scott Fahlman, a computer science and artificial intelligence research professor at Carnegie Mellon University, responded, "People may be shocked by some invasions and decide to forgo those things, while they don't notice themselves being engulfed by others. … We have to understand the specific threats and develop some social awareness and social consensus about how to deal with them."

Aj Reznor, vulnerability and network researcher at a Fortune 500 company, commented, "More people will connect, but a large portion of that may be unintentional, via devices that self-configure and phone home automagically. A consumer will likely only be concerned about a security risk if a close associate (family, coworker) is affected. Otherwise the old 'Why would someone want to hack me or my thermostat? What's in it for them?' mentality is likely to prevail."

Uta Russmann, communications professor at the FHWien University of Applied Sciences of WKW in Vienna, replied, "The majority of people do not understand the Internet of Things and what comes with it for them (data collection, etc.), but they see the amenities to be greater than inconveniences, so they will move more deeply into connected life. The physical damage to 'Joe Sixpack' will be very small; she/he will be primarily affected by it as all her/his data is stealthily used for marketing purposes (most people won't even realize this). I am more concerned about the general human damage: What about ethical aspects? Will there be enough people to question the doings of corporations, governments, etc.? (The fewer people who understand it all, the fewer who are in charge of the many.)"

Theme 3: Risk is part of life. The Internet of Things will be accepted, despite dangers, because most people believe the worst-case scenario would never happen to them

A number of participants in this canvassing noted that humans possess an inherent optimism bias when measuring risk versus reward. While they understand that connected platforms and devices can lead to negative outcomes, they figure the bad stuff will happen to someone else or, if they suffer in some regard, they will still land on their feet.

Eduardo Villanueva-Mansilla, associate professor of communications at Pontificia Universidad Católica del Perú, wrote, "The wonders of the IoT will prevail even against the risks. Experience shows that most consumers tend to ignore the risks unless they happen to *them*, and even when something bad happens to anyone they tend to prefer to return to their old practices since they are accustomed to them. … The risks of the IoT seem farther away from consumers than the everyday risks of getting mugged, so unless there are massive losses of money the problems will be incorporated into everyday risk assessment and forgotten in favor of the benefits."

David Durant, a business analyst in the UK Government Digital Service, said, "Even if there is a 'mass hack' of such platforms people will very quickly return to using them in the same way they returned to airplane or subway travel following terrorist attacks."

Adrian Hope-Bailie, standards officer at Ripple, said, "The allure of better services will always be stronger than the fear of the risks. … There will be breaches and dips in trust but the overall trend will be strong growth."

Richard Adler, distinguished fellow at the Institute for the Future, replied, "Despite continued security problems, the IoT will spread and people will become increasingly dependent on it. The cost of breaches will be viewed like the toll taken by car crashes, which have not persuaded very many people not to drive."

An **anonymous professor at New York University** wrote, "Compare automobiles, which reliably kill tens of thousands and injure millions of people every year in the U.S. alone. Now ask yourself how many people opt out of owning a car."

An **anonymous research officer** said, "People are willing to embrace life-altering technologies as long as the risks of use seem reasonably mitigated. This is true for everything from planes and existing automobiles to cellphones and debit cards."

David Sarokin, author of "Missed Information: Better Information for Building a Wealthier, More Sustainable Future," said, "I can certainly see the emergence of a 'Live Unplugged' movement – people who get mostly or completely offline, motivated in part by concerns for safety, but probably more for a desire to live the simple life. But unplugging from the internet will be even more difficult than unplugging today from the power grid. People will do it, but not in huge numbers. The fact that hundreds of millions of credit card files have been stolen from major companies hasn't seemed to affect credit card use in any significant way (other than spurring the use of those dammed chips). I expect people will respond with similar equanimity (or is it resignation?) as other issues emerge."

An **anonymous respondent** observed, "We are quite capable of compartmentalizing life, holding opposed thoughts in our minds with an easy satisfaction. Think, for instance, of people who complain about technology, while driving cars, flying in planes, being mended by laser surgery, etc. Or consider creationists who fail to eschew the products of modern science. We should therefore expect to see people shunning one aspect of the Internet of Things, while continuing to use networked devices for others. I'll get mad at people spamming my fridge, but still use Twitter to complain about it. Someone else will be disturbed by ads coming from their car's tires, yet still drive the vehicle to meet the date they met online. There's just too much of modern life immersed in the digital world to give it up."

Garland McCoy, president of the Technology Education Institute, observed, "Cyberwars will rage at the edge of the electric grid for some time, causing massive disruption. But in the end, as bumpy as the ride will be, people will accept the significant benefits of an always-on, connected life."

An **anonymous professor at a polytechnic university** wrote that people assume "the net benefits will outweigh the harms. We have seen how individuals sign hundreds if not thousands of 'terms of agreement' without reading them, how people give up personal data for enjoyable or useful services (Facebook, 'Pokemon Go,' etc.). People want to trust institutions and products."

An **anonymous respondent** commented, "Most users are going to assume (perhaps correctly) that they aren't going to be high-value targets for that kind of crime and will not worry too much about it. The pressure to increase that connectivity will likely increase and it'll just get even more onerous to disconnect from it. If you need to buy a TV, and all but one model are smart TVs, and most of the smart TVs make it really hard to not connect to the internet, most people are going to end up with a smart TV connected to the internet whether or not they actually wanted that."

An **anonymous computer scientist** observed, "Most people don't know or care much about the risks, however well known. Look at how they eat, if you want evidence. The biggest risks are 'tail

risks' of rare outlier events (e.g., a war in which your digital infrastructure and data is damaged, destroyed or taken over)."

Some respondents draw on history's lessons to make the point that people embrace new and valuable things, even when there are risks involved. An **anonymous system administrator** said, "Accidents will always happen and they will be contained only by the actual interface between humans and their artificial environment. For instance, electrical networks are quite dangerous but they have all kinds of fuses and fail-safes to prevent massive disasters. The digital systems that don't provide damage-limiting features will disappear. Not until after creating some disasters, of course."

An **anonymous respondent** replied, "Minor comforts in day-to-day lives beat basic safety. There was a decades-long lag between the introduction of cars and well-enforced speed limits, it took more decades for sober driving, and even more for basic safety items like seatbelts. People drove anyway."

Giacomo Mazzone, head of institutional relations at the European Broadcasting Union, commented, "Despite the growing number of incidents and hackings and problems related to IoT, the connected world will continue to grow. It will be like at the beginning of the introduction of cars. Society – in exchange for the advantages – will raise its level of tolerance and accept a higher number of accidents."

Dave Kissoondoyal, CEO of KMP Global, said, "The Internet of Things will make *all* connected. As the users and the providers have influenced the development of the technology and non-technology aspects of the internet, the Internet of Things will go through the same process. As more and more people have been trusting … the internet and connecting to it, the same will apply to the Internet of Things."

An **anonymous researcher at the Karlsruhe Institute of Technology** said, "Given previous reactions to security issues, it seems like users' tolerance towards threats is rather high. However, there is also a chance of a 'Data Fukushima,' a drastic event like the [Edward] Snowden leaks, that might lead to a new 'offline movement.'"

An **anonymous respondent** observed, "Whether one chooses to disconnect or not, they're still impacted in the event of major cyberattacks (e.g., power grid, SCADA [supervisory control and data acquisition] systems, etc.). That aside, if people are taking a more narrow personal view (e.g., is 'my' smart TV or car going to get hacked), it feels like an odds game – the chances that I would get singled out in a group of millions is small (and therefore why not just be deeply connected)."

A number of experts pointed out that most people don't understand the risk, which makes it impossible for them to accurately gauge risk versus reward.

An **anonymous IT architect at IBM** replied, "Most people will unwittingly embrace the Internet of Things because, frankly, they are too uninformed (and in some cases too stupid) to know any better. We already have auto manufacturers selling vehicles that must be accessed via proprietary, un-testable protocols, which are highly vulnerable to hacking. When will people wake up? I refuse to drive a vehicle with any sort of troubleshooting interface beyond a strictly physical one. I plan to buy a non-'smart' refrigerator and dishwasher soon so that I'll be able to maximize my use of them before one cannot buy a disconnected appliance. I do not need to install some app on a smartphone and remotely actuate my dishwasher. Sorry folks. I do not need to see how many ice cubes were ejected on a given day. This is just inane. Worse, I cannot trust the manufacturers of such devices not to send information back to the mother ship. Information such as frequency of use could easily correlate with absence from the home, such as for vacation. That is, if one's live vacation pictures posted to Facebook don't tip off perpetrators first."

Tim Norton, chair of Digital Rights Watch, wrote, "I don't think it will cause people to disconnect for the simple reason that generally, people are not aware of what the ramifications of attacks on IoT devices are."

Don Philip, a retired lecturer, replied, "Most people will be more deeply connected than they are today, partly because they will be unaware of the potential threats posed by the poor security that currently surrounds the Internet of Things. Physical damage could include traffic disruptions and attacks on homes and hospitals. Physical systems like traffic lights and hospital instruments could be shut down. Governments *could* act to make things more secure, but, based on current patterns, will probably work hard to install spyware and back doors, making things much more insecure. Technologists will be forced to go along. While it's theoretically possible to make physical IoT objects safer the vast majority of the time, as noted above, governments will work to subvert this, making things very insecure indeed."

An **anonymous respondent** commented, "People will become more connected. It is easier than ever to ignore reality and immerse yourself in what you want to see with the internet. People are good at choosing ignorance and staying ignorant, and threats against the digital life many treasure is something many will choose to remain ignorant of until it's too late and staring them in the face."

An **anonymous journalist, editor and author** wrote, "People will complain about the risks but feel helpless to avoid them."

Theme 4: More people will be connected *and* more will withdraw or refuse to participate

A portion of these respondents – 15% of them – said they expect that some people will choose to become more connected in the future, while others will opt out of the hyperconnected life. But most who articulated this theme said they feel that more will connect than will disconnect. Some predicted a trend in which some people become more connected at first and then pull back after serious IoT-connected infrastructure problems arise. Other respondents scoffed at the potential for the IoT advancing much by 2026, saying the technology will not be ready to be widely adopted.

Some will embrace it and some will 'opt out before it happens'

Some respondents predicted that the future will be a mix of those who buy into full connectedness and those who partially buy in and partially opt out. **Kjartan Ólafsson**, head of the department of social sciences at the University of Akureyri, Iceland, commented, "I doubt that being 'disconnected' will be a viable choice in life. People might have a choice of various levels of connectedness however and some people might opt for (or aim for) some kind of limited connectivity."

Steven Polunsky of Spin-Salad.com commented, "The marketplace will make Internet of Things a reality and people will have little choice. Eighty percent will adopt, actively or passively. Twenty percent won't, either, because they choose not to or because they can't afford to."

Ryan Hayes, owner of Fit to Tweet, commented, "I agree that both will be trends. More people will disconnect but even more will become significantly more connected. I saw Amanda Palmer speak at SXSW and she made a comment related to this that stuck with me: 'The most punk thing you can do today is disconnect. If you really want to be punk, go throw your phone in the lake.'"

Karl M. van Meter, sociological researcher and director of the Bulletin of Methodological Sociology, Ecole Normale Supérieure, Paris, wrote, "I cannot mark both 'Most people will move more deeply into connected life' and 'significant numbers will disconnect,' but that is what is happening and will continue to take place during the next decade. There will be great discrimination concerning for what being 'connected' is better than being 'disconnected.'"

An **anonymous senior security architect who works for a non-U.S. national telecommunications provider** said, "Disconnection seems to imply fully unplugging. I simply expect a relatively low rate of adoption over the next five to 10 years, rather than seeing people move more deeply into connected life. Greater adoption will lead to real headline-grabbing incidents unless the security and privacy of these solutions is given more thought. 'Fail fast' is not a recipe for

success when playing with other people's security cam footage, their remotely lockable front door or the self-driving function of their car."

An **anonymous respondent who works in government** said, "I would have answered 'Both.' There will always be a segment of society that understands and rejects the 'Big Brother' parallel."

David Golumbia, associate professor of digital studies at Virginia Commonwealth University, said, "Many more people will connect, and hacks, attacks and illicit algorithmic control will increase. Most people won't understand this and will do nothing about it even when it becomes clear."

George McKee, a retired research scientist who began online in 1974, replied, "People will become more connected, like it or not. Utopian dreams of happy, healthy, disconnected societies will be fulfilled only in isolated groups, like the Amish and the Mennonites."

An **anonymous futurist and impact investor** commented, "The answer is yes to both options. There will be a 95/5 distribution with most opting for connection, with a relatively large group – 5% – trying to live in the 'real' world. This will only last a few decades, however. Eventually we will all be connected."

An **anonymous principal security consultant** wrote, "Both of these are likely true, in fact. There will likely be many people who want to stick with non-connected devices for one reason or another, but most people will likely adopt them for the ease of use and convenience features. Outages are treated as the price of doing business already: If a major ISP or power supplier has an outage, it already causes significant problems, but customers are used to this and rarely cause significant trouble for a supplier. It seems likely that this will continue, at least in regard to non-critical equipment: If your smart light bulbs don't turn on or they flicker repeatedly it's annoying, but not the end of the world. Some people will choose to avoid this problem entirely and others will choose to put up with it."

Ed Lyell, professor of business and economics at Adams State University, said, "I believe many more people will choose to disconnect from the increasingly interconnected world. Yet the majority of people will accept and even embrace the Internet of Things since it will make their lives easier and more comfortable, perhaps even saving money. Yet criminals will also do well and hacks will occur. People are like water or electrical circuits and follow the path of least resistance. Thus, going along with industry-designed changes will be acceptable to most."

An **anonymous web and mobile developer** commented, "These threats are an evolution, a transition, of existing threats. As with every evolution, good and bad things evolve. There will be some time needed for people to adjust and take adequate security measures."

An **anonymous network architect at a major international telecommunications company** said, "It's just starting, and security implications have not been thought through enough. There will be a huge uptake at first, then some well-publicised disasters, and people will withdraw until a more secure second generation evolves."

Adrian Schofield, an applied research manager, observed, "Both answers apply. Millions will connect because they are at low risk and the convenience factor is high. Thousands will disconnect because they become targets or they fear becoming targets. However, fear of losing wealth has never stopped the relentless pursuit of wealth."

An **anonymous respondent** replied, "Major attacks, etc., may put a significant number of people off using these technologies, but after a certain point it will become impossible to fully participate in society without them. Perhaps a greater number of people will form alternative low-tech communities."

An **anonymous executive director for an organization advocating digital rights in Europe** wrote, "There is a big gap between 'most people' getting more connected and 'significant numbers' disconnecting. The correct answer is likely to be in that gap. Companies are desperately trying to connect *everything*, in the hope of harvesting useful data – from Bluetooth toothbrushes to period blood receptacles. This massive flurry of activity will take years to settle down and we will need to have worked through numerous scandals of data leaks and discrimination before we will be able to answer this question in a meaningful way."

An **anonymous professor of media production and theory** observed, "The question seems to suggest a kind of opt-out movement. It's possible. One thinks of the 'back-to-the-land' movements of the '60s. That kind of disconnecting might come in the next generation, one that sees real losses in terms of human possibility from over-engagement with the Net. And that seems remote. People love being bathed in concern, even if it is only via a Fitbit. The smart home is just around the corner, and the smart self-driving car is a reality (and the first fatal accident in one)."

An **anonymous respondent** responded, "People will not willingly or voluntarily disconnect. They may modulate. A little. But they will not disconnect. Look, families stay together even when the families are demonstrably dysfunctional and the individuals in them recognize and agree to the dysfunction – even when it's mentally and physically abusive and harmful to stay together. Look

what it takes to disband a family that objectively 99% of people would agree needs to be disbanded. This doesn't make staying together right or good. It just is. Social bonds are strong. Very strong. Electronic connections – they're just an easy, relatively cheap, diffuse, pervasive, ubiquitous way to maintain and manifest social connections. It doesn't mean that people won't also seek collectively effervescent experiences – raves, concerts, sporting venues. It doesn't mean they'll forgo physical contact. Or going to restaurants. But they'll also maintain their own social networks/connections *in* those venues. Disconnect? Ridiculous."

An **anonymous** respondent said, "Never mind personal privacy being violated or the risk of fraud. Over time, we will grow hardened or thick-skinned to these possible penalties of connectivity."

Right now the IoT isn't that grand, so why worry either way?

A number of respondents – most of them thinking mostly of consumer-oriented applications of the IoT such as "smart-home" items rather than the key global infrastructure for sectors like transportation and finance – said it certainly doesn't appear to be likely to provide much value to individuals. **Cindy Cohn**, executive director at the Electronic Frontier Foundation, wrote, "I think the Internet of Things is being wildly oversold and most of what they are building people won't want – not because of ransomware, just because they are dumb ideas. What I hope is that people will demand better security for the things that they do find useful."

Paul Dourish, chancellor's professor of informatics at the University of California, Irvine, commented, "Being able to remotely check the contents of one's fridge or switch lights on and off with one's phone simply aren't terribly compelling applications."

An **anonymous executive manager at an NGO** replied, "Currently, the IoT is more like a cargo cult than anything fact-based. Over time, areas where connection offers benefit will become clear, and areas where risks outweigh gain will also become obvious and die off. There are going to be horrible, horrible errors made and a great deal of damage done."

Several other anonymous respondents agreed, saying that in the short term many flawed or irrelevant IoT devices and systems will disappoint consumers:

- "The improvements in one's life from the IoT are nominal and not worth the risks. I want to use technology to fix real problems, not to tell me when I need milk."
- "Lots of people are already turned off by the connected home and other IoT BS. I could foresee a robust marketplace for 'old-fashioned' consumer products that just do something really well

without the bells and whistles. For example, a dumbed-down smartphone with limited icons on the screen, or a car with push-button interfaces instead of a touchscreen operating system."

- "Current corporate practice related to device support (i.e., the mass deactivation of devices made by the company Nest) doesn't encourage people to depend on these systems."
- "My dream is that highly connected vehicles will make cars less attractive as products as minor electronic glitches render them inoperable and unfixable and mass transit will become more attractive. It could happen, right?"

Another **anonymous respondent** observed, "In my view, the problem is technology that puts the user in a place of dependence on a third party. If a user doesn't trust that third party, that technology does not serve their needs. A key step toward establishing this trust is creating free and open source software (FOSS). One example of this is the mobile encrypted messaging app Signal. However, since software often uses servers that users do not control, there is still an element of trust needed. In the end, I think users will judge the IoT just like any consumer product and choose products that are a net positive. Just like the litany of $19.99 exercise equipment bought from TV infomercials, many IoT devices and services will end up in literal and metaphorical dusty attics."

A few of these experts argued that the hype around the Internet of Things would have the lifespan of a fad and eventually fade. An **anonymous participant** wrote, "If people begin to disconnect (as many likely will), it will be because they crave the desire for simplicity and occasional solitude. Once more people take the internet for granted, they'll use it more sparingly for the few things they truly need. Those weird buttons from Amazon that reorder laundry detergent for you don't add enough value for the average person. Maybe I suffer from a lack of imagination, but there is a limited utility to the Internet of Things except in certain circumstances."

An **anonymous respondent** predicted, "This one won't work out. This is a fad to 'connect' your toaster to your toilet. People may actually learn that having your front door locks connected to the internet is a very bad idea, and that keys are pretty great after all."

Another **anonymous respondent** agreed: "The term 'connected life' is unfortunate. The term 'connected world' is a fad. People were always connected with others. Let's go back and read Alvin Toffler."

Theme 5: Human ingenuity and risk-mitigation strategies will make the Internet of Things safer

A large share of these experts wrote about the ways in which solutions might be found to mitigate the risks posed by highly connected life. Some expressed hopes that market forces might punish Internet of Things creators if they do not build safe and reliable products and come to an agreement on appropriate system standards. Some predicted there will be consumer protests that might shame makers of shoddy products. Others expressed the hope that the ever-evolving code underlying the IoT and its connected items will be intentionally aimed – as a first priority – at security, safety and human rights while keeping up with the emergence of negative exploitations of the IoT. And they predicted that there may be solutions that could wall off mass-scale attacks on the IoT.

Effective regulatory and technology-based remedies will emerge to reduce threats

An **anonymous vice president of global engagement** replied, "The hacks and attacks to come will be followed by market-driven and regulated demands for increased security and resilience measures, rather than people deciding to disconnect."

Robert Bell, co-founder of the Intelligent Community Forum, wrote, "Sooner or later, there is going to be a significant wave of cybercrime that makes every company in the ecosystem and every user wake up to the dangers. We may see a step back at that point, but I have confidence that services providers on one side and the users themselves will find solutions that strengthen security online. It unfortunately takes a crisis to make people care."

David Karger, a professor of computer science at MIT, said, "As it becomes ever easier for computers to kill people, I do expect a dramatic increase in pressure on people in the computing industry to develop more trustworthy and reliable computing systems. There are ways to do that, but they come with costs in time, effort and money that haven't yet been seen as worth it. I do expect some highly visible and severe incidents to occur, but I expect that people's chronic preference for fun/convenience over safety (consider the number of people who still smoke, ride motorcycles, play football, etc.) will continue to drive adoption of risky but convenient IoT technologies."

Brian Behlendorf, executive director of the Hyperledger Project at the Linux Foundation, wrote, "A greater premium than before will be placed on systems that are resilient to failures of different sorts; are focused on individual sovereignty (e.g., personal control over personal technology, if not control over one's personal data); and are interrogatable (able to answer the question of 'why' – why it did a certain thing, or recommends a certain course of action). Those greater premiums may be

expressed in the form of regulations, or in lower insurance premiums, or in new consumer meta-brands that operate like 'organic' did."

An **anonymous associate professor active in wireless research** said, "The Internet of Things is a cyberphysical security disaster in the making. Think Sony Pictures (the company was being run by North Korean-employed hackers for some weeks) times 50 billion networked things. Now that is a disaster movie I never want to see. These IoT risks will lead many sensible people to be very wary of the first-generation crap now on offer by Silicon Valley Unicorns and the usual-suspect firms. A new model for cyberphysical system security is needed if it is to be advisable for people to have faith that Internet of Things devices and objects are safe to use and can be relied upon. Fortunately, some of us have been working on such a model for 15 years. The Open Specifications Model for Wireless Grids in the Internet of Things version 0.4 was released in the fall of 2016, incorporating blockchain, military-grade, embedded system security mechanisms and role-based access control to make the Internet of Things safe. We hope :). The most likely damage is that which is present today, where malware and specifically ransomware takes over carelessly guarded or unprotected systems."

An **anonymous professor of computing** observed, "Different devices can cause different damages (e.g., cars can crash, but a toaster cannot move). Since there is no universal technique for guaranteeing the safety of disconnected devices, it is unlikely that we will be able to develop such universal safety techniques for networked devices. Nevertheless, Underwriters Laboratories does a good job of certifying disconnected devices through experimental measurements. Perhaps a similar experimental approach could be used to certify networked devices as well."

Susan Price, digital architect at Continuum Analytics, wrote, "I do hope that blockchain technologies and user-empowering identity and data management platforms will emerge to enable users to have a better understanding of the value of their data and give them opportunities to monetize it – or at a minimum, a much more sophisticated awareness of its existence, who has access to it, and its uses. Hacks, ransomware and so forth will continue to be a game that we play, but the market will generate fixes and provide services to continue to allow people to participate online. There's too much potential benefit for citizens and vendors for such activity to cease."

An **anonymous respondent** commented, "We need to throw a lot of engineers at it and perfect AI learning engines aimed at real-time safety systems when objects interface with humans."

Joan Noguera, a professor at the University of Valencia Institute for Local Development, replied, "Prevention mechanisms (anti-hacker, anti-virus, etc.) will most probably be improved, thus diminishing the risks of connectivity."

Jeff Kaluski, who did not share additional identifying details, commented, "Trust is going up as security vulnerabilities are being found and patched; hackers are having a harder time once the potential pitfalls are published. Open source will be the path that the IoT will be secured along."

An **anonymous principal at a communications consultancy** with previous top-level experience at several of the world's top technology companies said, "Government must work with the tech sector on smart solutions for better security. And yes, it is possible to network objects that will generally remain safe for the vast majority. That's the case now."

Isto Huvila, a professor at Uppsala University, wrote, "Natural disasters and human action are the most likely threats. The best possible way of securing connectedness is to see to it that systems are autonomous, regional and local and do not rely on the functionality and presence of specific global infrastructures. That online systems can function on a municipal, regional and country level, [assuring] that infrastructures do not rely on each other."

Ray Schroeder, associate vice chancellor for online learning at the University of Illinois, Springfield, commented, "The Internet of Things will continue to rapidly grow and become more reliable with time. Connectivity and networking will become the lifeblood of effective tools and technologies. Systems will be hardened against intrusion and disruption. While hacking battles may persist, effective technologies will continue to adapt and advance to remain one step ahead of the black hats."

David Morar, a doctoral student and Google policy fellow at George Mason University, replied, "If engineers and policymakers are able to create infrastructures and standards that prioritize privacy and security, the future will be slightly less dangerous. If one examines technological innovation, the most glaring thing that pops out is that path dependency plays an important part. If the initial steps are not guided by what can already be identified as potential future issues, then the work of mitigation and consolidation later on will be much more difficult. A total reliance on connected software for almost everything in our lives will lead to a significant dependence on technology. After a few generations of such dependence, a critical failure in the system would nearly cripple the world. Thus, another concern that should be addressed would be to prepare for a temporary shutdown of our connected systems, just like we do now for potential power outages."

Thomas Keller, head of domain services at 1&1 Internet SE, based in Germany, and active ICANN leader, wrote, "The train cannot be stopped anymore. Technology providers need to be aware of their responsibility."

John B. Keller, a director of eLearning, said, "We need override capabilities and firewalls that will keep contamination from spreading virally. This is especially important in any system that could be directly or indirectly associated with human safety (e.g., navigation, air quality, water quality, food safety). We must have ways to minimize the opportunity that such systems would be compromised and should insist on designs that allow for quarantining to mitigate the effect of malicious or inadvertent corruption."

Erik Anderson, who did not share additional identifying details, replied, "Devices will always have vulnerabilities. You must stop investing [only in] firewalls and other perimeter security. You must add security at the data level. Secure objects that remain secure regardless of whether they are in motion or at rest. Look at Constructive Key Management (CKM)."

LT Wilson, who did not provide other identifying details, said, "We'll collectively learn as we go. Advances and vulnerabilities and fixes will successively ladder up."

An **anonymous executive director at a major provider of open source software** observed, "Most of us will become more connected – and we won't see the trade-offs – privacy, security, personal agency, risk of failed systems. At some point, market actors will emerge to give people a connected life with fewer trade-offs and more control. But this will take a long time."

An **anonymous managing director** replied, "Better underlying infrastructure – in hardware and software – will be developed (two steps forward, one step backward, but progress will be made). Better systems will be developed to limit the damage. It will remain a cat-and-mouse game. If populist governments are able to use the internet (via Facebook, Google, etc.) for their hideous purposes, things will change and people will become far more careful."

An **anonymous professor at a major university** commented, "Technology companies will respond to threats by making connected devices more secure. They will tout this security as a competitive feature of their products."

Michael Dyer, computer science professor at the University of California, Los Angeles, said, "I am not a networking expert, but researchers in networking are developing distributed systems that produce quality of service while remaining robust under a wide variety of perturbations."

An **anonymous executive producer and creative director** commented, "Theft of money, data and identity. Attacks on the government by other nations and organizations. The solution is to create the best super-intelligent AI at any cost and have its interests aligned with ours."

Ed Dodds, a digital strategist, wrote, "Most 'hacks' are still a case where a database administrator is on two payrolls at once (i.e., thumb drives walk). Government IT contractors will continue to classify unnecessary amounts of materials at a 'top secret' level so as to make their services appear indispensable and un-auditable. Private software-defined networks are likely to proliferate as a means to limit some outsider access to the connected sensor grids."

Dariusz Jemielniak, professor of management at Kozminski University and Wikimedia Foundation trustee, said, "Current technology already offers much higher levels of security than the market actually uses; there is a scope for radical improvement if people demand it."

Malcolm Pell, an IT consultant, observed, "Too many manufacturers, OEMs, developers see effective security as a cost burden. Also, how do we maintain the security of legacy and unsupported and obsolete devices?"

Barry Chudakov, founder and principal at Sertain Research and StreamFuzion Corp., replied, "Sanjay Sarma, [MIT professor and] one of the fathers of the IoT, points to a potential cause of networked-object damage when he says there are too many standards and not enough commercial, academic and government coordination to help create a dominant IoT architecture: 'Outside of a few exceptions there are no toolkits and everything is open-ended.' … Manoj Saxena, executive chairman of Cognitive Scale, says computers are super-intelligent, they are not super-conscious. It is now incumbent upon us – and of course the creators of the Internet of Things – to bring awareness and consciousness not only to the objects we use, but also to the people who use them. This is something for which we are mostly unprepared. … The way to network physical objects in such a way that they will generally remain safe constitutes an entirely new industry, or at least a sub-industry: communicating about the nature of connected objects (how do they think and what does that thinking mean for you); explaining hidden functions and processes or making those functions and processes completely transparent; and enlightening the users of those objects about possibilities and dangers. … Sarma posits three important steps for making things more secure and safe: 1) agreement on a system architecture, 2) development of open standards reflecting the best architectural choices, and 3) creation of a DARPA-like test facility where best practices can be designed and perfected."

Adrian Hope-Bailie, standards officer at Ripple, said, "The vendors who provide Internet of Things services to users will be measured in some way on how well they protect their users, so market pressure will force them to continue to try and stay ahead of the curve with respect to security."

David Williams, who did not share additional identifying details, said, "We are in for a rocky ride. There are sure to be many very high-profile cases of that connectivity being abused. One of the bigger challenges we're faced with is how to ensure all those new connected 'things' are connected securely and yet able to be safely updated as new bugs and vulnerabilities are found. Things like Wi-Fi access points and cable modems are cautionary tales as they often are tuned on, connected and never patched. That security patching has to be built-in, bulletproof and secure. Manufacturers need to have the cost of patching and maintaining those 'things' built into their costs, perhaps covered by a 'thing' annuity that would ensure funding for maintenance over the long haul and across mergers and acquisitions."

Ryan Hayes, owner of Fit to Tweet, commented, "It's true that our attack surface will just keep increasing as we surround ourselves with devices. but defenses are getting more capable as well (analogous to how people used to leave their houses unlocked when communities were more simple but today they have elaborate security systems and cameras, etc.). What I hope and expect to see coming into the market soon are more tools that use AI to study home network activity and identify anomalies instantly (so if your toothbrush suddenly starts sending large data files to some server overseas it flags and stops that quickly). Protecting home networks needs to be more of the focus as that's the big weak point right now."

David Krieger, director of the Institute for Communication & Leadership, based in Switzerland, commented, "System crashes pose a greater threat than cyber warfare or criminality. Much more work has to be done on data security, AI security, etc., which must be based on global governance structures beyond nationalistic self-interest. Techno-socially, engineering will become a question of 'design,' that is, accounting for all possibilities in the most efficient and aesthetically acceptable way."

An **anonymous director of human rights** replied, "People will likely have to actively choose to disconnect, meaning that many will automatically become more connected. Governments and companies should consider connectedness by consent instead of by default as a guiding principle, along with articulating clear and effective privacy protections and safeguards – including greater liability for private actors involved in serious privacy breeches."

Several respondents expressed the hope or expectation that global technology companies will become more willing to be transparent about their processes, security and other aspects of connectedness important to the individuals they serve.

An **anonymous president of a consulting firm** replied, "Transparency will emerge regarding who has the best interests of global citizens at heart, and who is a manipulating mercenary. The

politics of control and the politics of appearances will give way to the politics of transparency, which will force corporations to do the right thing for humanity regardless of whether they want to, or not. The sheer volume of discounts made possible when hundreds of millions participate creates a whole new set of global dynamics ripe for innovation. The battle between good and evil will continue online. At issue is which side the majority of the global population makes the choice to join based on personal values. The dire need is for everyone to understand how to achieve a win-win for all citizens globally to actively participate in the interconnected global economy."

Chris Zwemke, a web developer, said, "The Internet of Things is but a giant playground. As people become more and more aware of security and algorithm dangers, the bar for what is a useful 'thing' will continue to rise. … What we connect to will shift. People will realize the safety perils of cameras and interconnected cars. The age of having dozens of devices on Wi-Fi will come to an end before the decade and a superior, secure wireless format will emerge. First from a consortium of the typical large industrial players (Google, Apple, Microsoft, Verizon, AT&T, GE, etc.) but it will morph into a regulated space, much like television and radio. I have no idea what the answer will be, but there will be one. Once the secure and trustworthy communication is found and proven, the rise of smart cars and appliances will start in earnest. However that rise is more than a decade away. In the same time span, culture will realize some of our connected things are in fact dumb – the smart toothbrush – and the utility of connected things will rise. Perhaps a hurdle of regulation and openness will force the lesser-quality actors out of the field and into the black market where they won't have anything more than a pestering impact."

Some respondents speculated on ways in which individuals might handle taking some control of personal safety.

Cristóbal Palmer, technical director at ibiblio.org, commented, "People are likely to get more sophisticated about segmenting networks, using distinct personas for different devices, and other steps to mitigate the risks associated with what some call 'The Internet of Unpatchable Crap.'"

An **anonymous** respondent wrote, "Some sort of 'airplane mode' will become more common, and a sizable minority of people will use it regularly, but most will not disconnect entirely."

An **anonymous system analyst** commented, "I think that, in fact, people will choose to create some kind of 'disconnection sanctum,' maybe a corner in their house, or an office, or even going into a cafeteria, time after time, where they'll give away their connections and stay offline for a while, so they can "breathe in."

An **anonymous respondent** replied, "People who see their only option as being exploited will disconnect from whatever is exploiting them, once they learn what's really going on. … Everything depends on the quality of mentorship, training, and ongoing support within a trusted support network working to limit online risks and maximize online benefits requiring the least investment in time, energy, cost and prerequisite literacy."

Will Kent, an e-resources staff member at Loyola University-Chicago, used a historical reference to early mail service to introduce more-modern measures needed today, writing, "Two hundred years ago we were able to make mail safe enough to become the relied upon technology for all sorts of information (health care, social, civic, economic, etc.) so it seems like there should be a safe digital analogue in the technology somehow. It may take business embracing privacy in order to do it (like the government respecting privacy with physical mail). It will also take coordination and de-centralization to preserve balance, back-up and adaptive support to ongoing threats with developing technologies. Lastly, and most problematically, it will take the vigilance of users to demand protection, oversight and transparency. This is the only way we will be able to fix damaged devices in networks or reconfigure things on the fly or call out attackers. As it stands, this conversation is over and things will become more connected. Authoritative bodies must advocate for user education and safety. Even if this is a priority for some, it is not a common practice for all."

Edward Friedman, emeritus professor of technology management at the Stevens Institute of Technology, replied, "These new technologies will not emerge overnight. As they evolve, people will have an opportunity to evaluate them and adapt to new connections in a judicious fashion. The technology of safeguards will also be evolving and becoming more effective."

Additional **anonymous respondents** chimed in on risk mitigation:

- "People won't stop to think about risks they don't even understand."
- "Better responses to these threats will be developed once more people are involved."
- "With some basic precautions (VPN, SSL, HTTPS, good passwords), I can for the most part participate in the available connected life."
- "Vulnerabilities will delay but not prevent the inevitability of the connected life."
- "Problems resulting in injury or death will be addressed after the fact using best practices that are good enough for insurers."
- "While it is possible to improve safety, [a] sense of public responsibility needs to be aimed at the legislators and large corporations with the power to create better security."
- "More attention is being given to these safety issues by government agencies and efforts are underway to increase digital infrastructure security."

- "These systems will need to change from being cast in stone (not upgradeable with bug fixes and security fixes) to being upgradeable in the field."
- "Safety-critical systems will be [created], and hopefully will be designed to a higher standard and be 'fail safe.' In many cases the networking is just a gimmick and provides not real benefit (such as smart homes)."

Governments should be doing more to regulate negligent companies, punish bad actors

Many respondents called upon government to do a better job holding both the IoT companies that are building the systems and devices and those who perpetrate crimes accountable for their actions. Some said profit considerations are generally prioritized above security in the research, development and rollout of IoT-connected devices and services, and bad actors are often not penalized, from companies that are negligent in the creation of IoT products to criminals or crackers who take negative actions.

M.E. Kabay, professor of computer information systems at Norwich University, wrote, "The IoT will result in even greater numbers of systems compromised by criminals to create ever-larger botnets (networks of 'zombie' computers responding to instructions from 'master' systems). Botnets are used for generating spam (unsolicited commercial email), and especially for fraud. Use the search string < refrigerator used for botnet > for example. Distribution of malware such as ransomware is also facilitated by botnets. Botnets are also used for distributed denial-of-service (DDoS) attacks, in which targets are flooded with overwhelming traffic that can slow response time or even crash the targets. Some of the IoT includes controllers for critical infrastructure. The Stuxnet attack on Siemens centrifuges in Iran and other countries demonstrated the long-standing view of information warfare specialists that unprotected or under-protected supervisory control and data acquisition (SCADA) systems could be subverted to cause significant real-world damage, not just effects on information alone. Medical IoT devices are particularly significant when considering possible damage to people; so are connected automobiles, which have become computers with wheels. There are already many examples of how cars can be hacked at a distance; use the search string < car hacked crash > for reports. The fundamental issue is that security is an afterthought for much of the IoT; the manufacturers bear few consequences for misuse of their poorly engineered systems, so some managers elect to shift costs away from their development process and simply let consumers bear the brunt of the damages. The calculation is that they can pay less in fines than for better security. The notorious Ford Pinto exploding gasoline tanks is the classic example of this cost-shifting approach. There is *no reason* that IoT security cannot be improved; however, under the current economic system it is largely free from independent regulation. When IoT devices are subject to the same stringent requirements that pharmaceuticals must meet, we will see some reduction of risk."

An **anonymous respondent** said, "The IoT will increase the pervasiveness of 'transactional overhead' problems (e.g., adver-surveillance). The desire by IoT providers to preserve the supplemental commercial opportunities afforded by such unwanted side channels will make the IoT less secure, and thus contribute to more frequent and severe incidents over time, but these are unlikely to deter the vast majority of consumers from embracing the IoT more and more unless/until some profoundly disruptive and unavoidably high-profile incident interrupts the trend." Another **anonymous respondent** wrote, "The necessary incentives to employ and upgrade and maintain the highest security levels of the IoT, may not be able to be driven by market forces – it remains to be seen." And another said, "Online security breaches are going to be a pervasive part of life from here out."

Matt Hamblen, senior editor at Computerworld, wrote, "Governments in some countries seem on top of the dangers, but the U.S. government is clearly not up to the task and doesn't seem aware of the dangers or equipped to deal with them as there is a very small consumer protection establishment in place."

Evan Selinger, professor of philosophy at the Rochester Institute of Technology, said, "The issue of how much trust will exist in the face of heightened vulnerabilities likely will be decided on how effective government regulation is and how quickly it goes into effect. For example, in "The Internet of Heirloom and Disposable Things" [an article published in the North Carolina Journal of Law and Technology], Woodrow Hartzog and I argue that not enough regulatory emphasis is being placed on the different kinds of things that can be wired up online. In some cases, the different lifespans between IoT software and IoT objects can be staggering."

An **anonymous emeritus professor at a large state university** observed, "I see no signs that governments, as presently oriented and influenced, will even attempt to limit the harms that result from a connected Internet of Things. … Catastrophic failures will occur, and our responses will be inadequate, in part because a population that has become dependent upon this network will not be willing to shut it down."

An **anonymous respondent** commented, "Governments won't be able to do anything as long as they remain willfully ignorant about how these systems work, and they continue to attack security researchers, encryption manufacturers, etc. If they actually worked to create knowledgeable groups within government about technology/networks they might be able to create some headway by requiring security audits and strongly encouraging (or even requiring) FOSS software on network-critical points that might be able to interrupt some attacks. Technologists would need to critically assess what is going on, instead of assuming that there will be some sort of technological breakthrough (quantum computing for example) that will wave a magic wand to fix everything. Air

gapping is possible but would require a complete reversal of the present course. This simply won't happen in 99%+ of situations."

George McKee, a retired research scientist who began online in 1974, replied, "Governments will be compelled to step in with regulations regarding 'fail-safe' modes and for 'living will' provisions for security updates and continued operation of backend systems supporting internet-connected devices. This is unfortunately likely to happen only after serious injuries and lost lives occur."

Christine (Malina) Maxwell, entrepreneur and program manager of learning technologies at the University of Texas, Dallas, replied, "Cyberwarfare is real – major breakdowns are more likely to occur as the IoT goes 'mainstream.' There will need to be far more collaboration among governments and technologists to thwart ever-more-sophisticated cyberattacks. The public should be educated on the impact of the Semantic Web – and it should learn swiftly why it should be pushing for IPv6!"

An **anonymous vice president of product at a new startup** observed, "The big threat is the deplorable level of security in the Internet of Things ecosystem. … A combination of an industry standards certification approach like Underwriters Laboratory and regulatory oversight like the Consumer Product Safety Commission could help."

An **anonymous principal architect at Microsoft** wrote, "Increased use of IoT devices is inevitable – but many of these devices are negligently designed. Their designers will need to face civil and criminal liability before they clean up their act."

An **anonymous software engineer** wrote, "More people will be more deeply connected despite potential dangers. The system is not closed and will iterate to a balanced trade-off between benefit and risk. It's not possible to be generally safe with any technology and the benefits will not be worth either the risk or the cost of security, so use will be more limited than the hype suggests. Government intervention will be late to the party and mostly ineffective other than to assign liability. Technologists will have solutions but will be mostly ignored by management until there is liability risk to them. Naturally evolving standards in the marketplace can have a mitigating effect on security risks."

An **anonymous respondent** observed, "From my own experience, I have moved more into networking because it simply has become too much of a nuisance not to. I don't like it, though, and I don't believe it is very safe. A government approach to safety might involve a complex physical token that must be read along with a password. The Japanese 'inkan' seal might be the basis of such a system. However, could it be easily replicated by a 3D scanner/printer? It seems to me that flaws

and insecurity are inherent in digital computer technology and will get worse when physical systems are more inter-networked."

An **anonymous respondent** observed, "The Internet of Things is far more likely to manifest as a collection of unconnected wide-area networks – all the traffic lights in my town, not all in my country. Of course things will be rushed to market and products will be badly designed and poorly made (see any other innovation). Eventually there will be standards and hardening, physical and logical separation, etc. Early adopters like the Netherlands and Singapore are more likely to take a practical approach to implementation than places like the U.S. This means we'll end up with two standards – the global standard and the American standard. And they won't cooperate."

Another **anonymous respondent** replied, "It is not possible to run an open network safely. The internet was not intended for this and all the Band-Aids and new ideas they apply won't make it so. Either they have to lock down the internet so they can do this, or they have to give up on this to keep what is good about it already. Strict liability for *anyone* who holds data would be a good start. Ninety-nine percent of our problems are from organizations keeping people's private data that they have no legitimate need for, and then it gets stolen. Stop keeping the data, security rises exponentially and then other things might be possible."

A cohort of respondents talked about basic forces that might work to mitigate some key problems in the IoT space, but also added that they are not sure the perpetual fixes will ever enough to beat back bad actors. Some said no matter what happens, the threats accompanying complicated connected digital systems are never likely to be completely conquered.

An **anonymous respondent with the Internet Engineering Task Force** said, "The advantages [of the IoT] are compelling. But the risks are, too. There will be some major public failures. Hopefully these will motivate tightening up the systems so people can continue to use them. But the problems will not go away, just as crime never goes away in the physical world."

Chris Showell, an independent health informatics researcher, said, "I have argued in 'Risk and the Internet of Things: Damocles, Pythia or Pandora?' … 1) These risks should be viewed as similar in nature to ecological risks, and … the precautionary principle should moderate the widespread introduction and use of the IoT. Making these devices 'safe' will be almost impossible. A number of manufacturers and vendors pay insufficient attention to device security … and may even weaken security settings in the user environment. 2) Reliably upgrading the embedded security of these low-power devices retrospectively will be near impossible in a dispersed domestic setting."

Andrias Yose, a global freelancer, wrote, "The possibility to network physical objects in such a way that they will generally remain safe for the vast majority most of the time? Not very likely when humans with humans' self-will or self-determination are involved. The most likely kind of physical/human damage that will occur when things are networked [is tied to the things that] make humans human; personal security; identity theft; deep(er) self-reflection/introspection on things in general or of interest; national security threats. Governments and technologists respond to make things more secure and safe: more laws; more spying; more safety nets or safeguards; incrementally complex encryption and/or protection (also with loopholes), all of which will be created with unthought-of loopholes."

An **anonymous assistant professor at a U.S. state university** said, "This is the hardest to project. It depends on how public policy addresses the security of information online and the protections the governments provide from cyberattacks and the like. The federal government has struggled to develop a comprehensive policy to these ends, and if that continues, and cyberattacks intensify, it is likely that the government acts in response to any serious uptick rather quickly, preserving public trust. But ultimately it will depend on appropriate government action."

Theme 6: Notable numbers will disconnect

Some 15% of these respondents are not at all confident that the Internet of Things will be safe enough to command trust among users. They argue that a number of the problems mentioned elsewhere in this report will be severe enough that some people will retreat from super-connected life. They particularly stress how key systems such as health care and finance sectors as well as utilities and other critical infrastructure arrangements will likely be top targets of attacks by terrorists, national enemies and highly motivated hackers. They are concerned that the people behind the creation of the IoT are not willing to invest the resources needed to do the hard work of minimizing negative effects. Some see the primary motivation of builders of the consumer-facing IoT to be aimed mainly at the mercenary monetization of everything.

Lack of trust, safety and privacy issues and more may move those with fears to withdraw

Trust was singled out by a number of respondents as the most crucial factor when it comes to connectivity. Among those who see this as a prime reason for disconnection are those who also predict that it may become the reason behind an organized movement.

Raymond Plzak, former CEO of a major regional internet governance organization, observed, "Disconnect will happen [to some extent] as long as there continue to be cyber exploitations causing feelings of anxiety and mistrust."

An **anonymous respondent** said, "People will not want to be connected 24/7. Lack of trust will be a factor."

Several respondents predicted that those who were victims of abuse tied to the IoT will be the vanguard of the disengaged. **Eelco Herder**, senior researcher at the L3S Research Center in Germany, observed, "Most people will continue to move more deeply into connected life. At least they will until at some point people or governments will be personally involved in attacks, hacks or ransomware, or until the point that these dangers become very real and direct. Many people believe that this is bound to happen."

An **anonymous respondent** observed, "Online terrorism will become a [bigger] thing. Terrorism is powerful and people will respond in a number of ways including disconnecting."

Alf Rehn, professor and chair of management and organization at Åbo Akademi University in Finland, wrote, "Whatever can be hacked will be hacked, and some will opt out. Not a majority, maybe only a smallish minority, but still."

Author **Paul Lehto** replied, "With the Internet of Things, the capability of a jilted lover to make mischief by turning off power when the love interest is preparing for a date with another, to use a somewhat off-the-wall but colorful and illustrative example, will cause significant numbers to disconnect for peace of mind and privacy reasons."

An **anonymous respondent** said, "There will be a disconnection from the larger Internet of Things, but it might look more like switching from shopping at Costco and shopping at the smaller local ma-and-pa store. Kind of like the farm-to-table movement, where you can verify the folks with whom you are transacting."

Some predicted that those who are disconnected will be part of an organized effort by a zealous minority. An **anonymous respondent** commented, "Perhaps there will be a new movement of people who choose to disconnect from everything. Like living off the grid, but at a much more fundamental level. Going dark." And an **anonymous professor at a state university** said, "Most will be connected, but disconnection will become fetishized. It will be talked about the way that meditation is talked about today. I expect to see device-free and disconnection workshops and probably a whole disconnection movement in the near future."

Corporate intransigence, shortsightedness and misguided thinking create vulnerabilities

A large share of the respondents to this study who do expect large numbers to disconnect said most of the exploitable weaknesses in the Internet of Things at this point and moving forward to 2026 are likely attributable to the companies creating internet-connected products. Among the reasons they cite are the need for speed in a competitive market environment and the costs in time and money of building in and maintaining security.

George McKee, a retired research scientist, said, "'Secure out of the box' has been a slogan of cybersecurity professionals for many years, but it will not come to pass as long as 'first to market' and 'easy to use' take precedence in product managers' priority lists. Only the most talented of designers are able to make the secure way also the easy way. The 'Internet of Abandoned, Misconfigured and Subverted Things' will become a powerful tool for malicious actors."

Nigel Cameron, president and CEO of the Center for Policy on Emerging Technologies, observed, "We've gotten used to having our basic information hacked, but cyberphysical systems raise the stakes exponentially. I don't know if we'll achieve *de facto* security, but I do know we are very far away from taking the agenda seriously. E.g., as I have argued elsewhere, the chief information security officer should report directly to the chief executive. Corporate reporting is an index of risk seriousness, and at present is out to lunch on these questions. Pablums from governments (like the

latest cybersecurity commission appointed by the administration) won't cut it. On the other hand, short of a huge shift in public attitudes (cf. GMO/Europe; they can happen), opt-outs from mainstream culture will remain oddities."

An **anonymous software architect** wrote, "Security problems, which are already bad, will become more and more visible until we reach some kind of tipping point, hopefully leading to regulation of such devices and meaningful sanctions against vendors who ignore security problems. However, I expect a significant number of people will reject these devices regardless of whether their security improves."

An **anonymous respondent** replied, "Most companies manufacturing IoT technology will most likely continue to be more concerned with producing a product that prioritizes cost of entry and ease of use over security, if only because there is no monetary incentive for them to do otherwise. Until a lackadaisical approach to securing technology becomes a financial liability (though harsh fines) no progress will be made on this front. Data will continue to be leaked, breaches will continue to occur, and people will still buy into it regardless."

David Collier-Brown, who provided no further identifying information, wrote, "Our current security and maintainability is far, far behind the state that we need for networked security cameras and routers (today!) and for baby monitors and refrigerators in the immediate future. Unless we get people like Dave Taht (co-founder of the Bufferbloat Project) and Vint Cerf (Internet Protocol co-inventor, see "Sometimes I'm terrified by the IoT") being listened to, I expect a boom-bust cycle as vendors sell garbage and unhappy consumers discard it."

An **anonymous leader at of a global privacy organization** observed, "This is the least-positive outcome: People will disconnect. There is so much benefit to be had but those in industry are idiots at privacy and security so they are going to destroy its potential. I want a connected future, but I doubt that the industry leaders and governments, will let it happen in the most equitable way possible."

An **anonymous director of business appraisal** said, "The Internet of Things – unless strong cryptography is adopted – will die on the vine. Some always-connected devices will remain, of course, such as those connected with entertainment, but every bit of bad press about a hacked webcam or heating system will drive people away from total integration."

Glen Thomas, a computing expert, wrote, "IoT devices do not generally get security updates, so most will have vulnerabilities for most of their life – owners will not be concerned about this if they

appear to still function. Snappy Core could help with updates, but OEMs [original equipment manufacturers] need to have legislative encouragements to get their security act together."

Amanda Licastro, an assistant professor of digital rhetoric at Stevenson University, commented, "The college students in my classes are already taking themselves offline by eschewing social media sites and deleting their own content from corporate-owned platforms. Many are influenced by the slew of movies, TV shows and books that present satirical or exaggerated versions of our future through a lens of constant surveillance and corporate control. At the same time, we are all reliant on these tools – Google, Facebook, messaging apps, etc. – to communicate and organize. This paradox may cause a division in our society that replaces or supplants the current political parties."

An **anonymous freelance consultant** said, "Most people will choose the easier path of increased connectivity, but over time we will see public trust in government, corporations and markets continue to erode as more breaches of security come to light. Governments, corporations and markets are already suspect to increasing numbers of people, worldwide. Lack of effective security will further erode trust and increase discontent. Combined with job losses due to automation, this will not end well."

An **anonymous technology analyst at a major global networking company** wrote, "As only GAFA [an acronym for technology company imperialism – short for Google, Apple, Facebook and Amazon but it represents more than these] can make money from each new set of eyeballs, the rest of us weigh the cost of each connection and our authority/policy over it. The central issue is technologists do not provide the hooks to manage my identity and information against binding arbitration and any default table of authority. Technologists can provide tools to consolidate the various civic, family and industry authorities with UCC 1-308 citizen's ability to alter contracts. ;-) Today it is much more secure to divide and store information locally (from my fitness watch to a program on my computer) rather than let the cloud have it. Moore's law says fog computing will win over cloud computing."

'TMI' and less-than-stellar performance from complex tech systems will drive dropouts

It all may just get to be too much for people to handle, leading at least some to give it up. That's what some respondents said. Varied stressors, including information overload, complexity of IoT products, failure of products to perform well and other emerging negatives – often in combination with safety and privacy fears – will move people to withdraw to some extent from participation. The reasons can be as complicated as the systems some choose to escape.

An **anonymous user researcher at a major global news organization** observed, “The fact that we now routinely update software on our computers to patch should tell us everything we need to know about the Internet of Things. Do you want to update your toaster? No? Do not purchase connected devices. There’s another problem. If your thermostat connects to a remote server to exchange data about your home-heating habits, and that company goes out of business, the next may no longer provide the servers to support your connected device. You may suddenly find that your thermostat doesn’t work. We are creating needless systems of dependency on companies through the Internet of Things. And then there’s privacy. Let’s say, for example, you purchase a smart television. If a company is collecting the data about how often you watch your smart television, we may want to consider that their primary reason to exist is to make a few dollars, and that data represents a revenue stream. Unless consumers read their privacy policies and terms of service, they are remarkably disadvantaged in their relationship with companies. Maybe the television company wants to sell the data with your insurer, or sell your television habits to data brokers to find out how often you purchase products you see advertised on your favorite channel. If privacy is a concern, it’s a lot easier to simply buy a disconnected device. It’s difficult to foretell the future adoption of networked devices, but I see no strong indications that the adoption will fall. This is despite the many problems with digital security, the inherent dependencies such devices create upon for-profit companies, and the privacy risks that can be abated through simply disconnecting.”

An **anonymous respondent** said, “I have no desire to have a more deeply connected life. I’ve got all I can deal with right now and don’t want my devices to be telling me what to do without my asking.”

Another **anonymous respondent** commented, “People can best understand linear, i.e., simple systems. IoT brings an even more pervasive complex system into our daily lives. This trend together with the lack of sense to have good security will result in accidents and, potentially, disasters as transportation systems and health systems become increasingly reliant on IoT technology.”

An **anonymous technology writer** said, “The Internet of Things will flourish in some of its many application areas but I doubt that the ‘connected home’ is one of them. Building operation management makes sense for hotels and high-rises, but connecting home objects at random ‘to the internet’ is a real alphabet soup of protocols and systems, difficult to secure but also difficult to maintain, upgrade and repair. Safety won’t be what stops people, it will be the same fiddly disenchantment that stops many from, for instance, wearing athletic tracking bracelets.”

An **anonymous respondent** predicted, “We are not going to be able to disconnect, but poor systems will make people want to disconnect as much as possible, and job loss to technology will

mean people will try to slow adaptation to technology and come up with innovative ways to increase productivity. This will be very interesting to watch."

Additional **anonymous respondents** who believe significant numbers will disconnect wrote:

- "I already disconnect."
- "This is an easy question to answer: It's happening already."
- "Without major social and political change this looks to be the best way forward."
- "People will get more and more fatigued by online lives and retreat to only necessary online interactions."
- "Boomers will seek to disconnect."
- "I expect many people to try to disable the connectivity of many of their machines."
- "What I'm hearing from early adopters of IoT technology is that they are always trying to find ways to turn the internet connectivity off."
- "What will happen when you can't buy non-connected devices? Almost all Android apps I use want access to my camera and microphone and I have to grant it or I can't use the app. I'm trapped!"
- "I laugh every time I see an advertisement for a 'smart refrigerator.' Are people really that desperate for a little convenience that they would open themselves up to hacking?"
- "I do think significant numbers will disconnect, but fewer will be motivated by security fears than by negative online experiences and a desire for more-authentic, caring interactions."
- "The Internet of Things is going to lead to massive security breaches that will drive people away from being interconnected."
- "Major risks will cause a counter reaction by which significant number of people will disconnect."
- "As each item comes online, there's more opportunity for the bad guys."
- "I can't wait to see how many people die from the Internet of Things."
- "I will resist the IoT as long and as much as possible."
- "People will try to disconnect, only to discover too late that they're unable to."
- "Without trust there can be no real safety."
- "The safest network is a disconnected network."

Theme 7: Whether or not people disconnect, the dangers are real. Security and civil liberties issues are being magnified by the rapid rise of the Internet of Things

Many respondents to this canvassing said they are certain that there will be more attacks with more devastating results as billions more things and people become interconnected online and systems become more complex and difficult to manage. Some say these security concerns are likely to lead to regulation, although it might not take place until after a devastating attack or exploit. Even if an extreme "threat environment" does not emerge, some respondents believe that the protection of individual rights – of civil liberties – is greatly endangered by the Internet of Things, a world in which enormous quantities of granular data can be continuously collected, databased and analyzed, then used to form judgments about people, and to try to sell them things and ideas, and possibly even to manipulate them.

Threats are likely to turn into attacks and other acts, possibly some violent

Nigel Cameron, president and CEO of the Center for Policy on Emerging Technologies, observed, "The sky's the limit; if you can hack a Jeep from a basement QWERTY keyboard you can take control of a nuclear power station or an aircraft or have a million cars turn left on cue. In principle."

An **anonymous chief scientist** wrote, "Hackable systems (that is *all* of them!) will be the basis of Chernobyl-type events in the connected world."

Marc Brenman, managing partner at IDARE LLC, replied, "Failures will continue to occur, and grow worse. Cascading failures will occur. Cybersecurity will continue to be breached. Safety is illusory."

An **anonymous respondent who works in government** said, "A natural disaster or EMP [electromagnetic pulse] may very well cause massive damage that cascades into all connected systems."

Miles Fidelman, systems architect and policy analyst at Protocol Technologies Group and president at the Center for Civic Networking, commented, "Hackers will hack. Criminals will plunder. We'll lurch from crisis to crisis. It's not clear whether it's possible to make things more secure, or to limit damage. We may be facing a continuing arms race."

Thomas Claburn, editor at large at InformationWeek, replied, "Judging by the state of computer security today, there's no reason to assume things will magically get better by adding more devices,

particularly those that govern daily interactions like cars, alarm systems and medical devices. Imagine the harm that could be done by remotely turning on the engine of a car in a garage at night, flooding a home with carbon monoxide while the occupants sleep."

An **anonymous systems engineer working for the U.S. government** predicted, "For significant systems – public infrastructure, health and safety – the risk may be high enough to prevent widespread adoption."

An **anonymous senior design researcher** commented, "I worry about monopolies with code that is vastly distributed and controlling home systems failing, causing entire regions to become unstable due to a line of code."

An **anonymous professor at a state university** commented, "It's actually surprising that we haven't already seen major disasters caused by hacking, of the sort that would close down cities or states."

An **anonymous senior software engineer at Microsoft** wrote, "IoT security will be poor and it will become a target for cyberwarfare."

Charles Perkins, senior principal engineer at Futurewei, wrote, "Loss of freedom is a very significant threat. It is possible to maintain safety but it requires big investment in product development, as well as a realistic vision for the customers."

An **anonymous respondent** wrote, "The risk of totalitarianism will increase, as the power to control other people's lives goes up and is accessible to corporations and governments."

An **anonymous software engineer** replied, "Your average user sees exploits [hacks and attacks via networked devices] in the news on a regular basis. Recent court decisions say you have no expectation of privacy if your computer is connected to the internet. The combination of these would lead me to decide the potential gains are not worth being connected."

An **anonymous respondent** commented, "The most-serious vulnerabilities involve the most-capable players. They can use stealth or blitzkrieg tactics on systems like infrastructure that no one can escape. The technology of an independent lifeboat does not exist on Earth."

Tom Ryan, CEO of eLearn Institute Inc., replied, "The Internet of Things continues to grow, especially as new ways to connect machine to machine to automate provide more convenience. There is also a corresponding growth in industrial and governmental cybersecurity and international

cybercombat that are driving threats and responses. There will most likely be a major event that will occur due to the opportunities that the Internet of Things provides to people that choose to do harm. My biggest concern is something that cripples countries' infrastructure (electrical, communications, water, energy)."

Pete Cranston of EuforicServices.com commented, "There will be scares, genuine disasters, but the potential gains from interconnectivity are so great that we will continue to lurch into a future where we will have to confront issues of independent machine-machine decision-making much more actively. (This is also known as machine intelligence, but actually has more to do with interlocking algorithms exponentially increasing the complexity of machine response patterns.)"

Susan Mernit, CEO and co-founder at Hack the Hood, observed, "For many, these will be viewed as creature comforts and conveniences – until they don't work as planned. The Big Brother aspects of the Internet of Things really scare me. I don't want my self-driving car to control where I go."

An **anonymous CEO** commented, "I don't think it's possible to network objects together to ensure they remain safe – a hacker is always one step ahead."

An **anonymous respondent** commented, "The trend toward connectivity is irreversible, but there will be at least one major crisis where a widely used internet-connected thing is hacked/compromised with highly visible results that 'bends the curve' toward better security (primarily security practices) by vendors of internet-connected things. It's going to take one or more crises in order to change the current situation with respect to widely deployed exploitable vulnerabilities. The [incorrect] view of 'things' as *products* (especially consumer products) as opposed to *systems* is why the reaction to this sort of 'thing' security crisis will be different as compared to the current acceptance of the existence of vulnerability after vulnerability for internet-connected items that hasn't changed anything seriously [up to this point]."

The rise of the IoT and security concerns amplifies worries over civil liberties

Threaded throughout many respondents' answers were concerns about the rights of the individual. They said the threat level for civil liberties is on the rise as more of the world and the objects therein become networked, intelligence-gathering nodes in the Internet of Things.

Masha Falkov, artist and glassblower, observed, "Encryption is key to protecting devices and the information they hold within, especially as everything becomes more interconnected. Yet governments and marketers alike wish to weaken privacy and encryption in favor of greater surveillance capability. This puts everyone in danger. Devices on whose consistent operation lives

depend can be tampered with, sometimes by individuals whose sole purpose is just to see if they could, as well as terrorists and other people of malicious intent. I don't believe it is possible to have 100% security because our operating systems are always evolving as we search for greater potential to our tech. But it is possible to improve security through several means. One is to require high security standards and encryption on all connectivity devices, and to make companies that create these devices and software liable for damages that may result. This will ensure to some degree that companies do not skimp on their security teams. Another means, which is happening right now, is to enlist hackers into helping companies and developers into finding security flaws through the use of cash prizes or employment. This also creates an outlet for people who love to hack to be productive individuals rather than a nuisance. Finally, make sure that the laws are set up so that hackers who find flaws but do not exploit them can report them without fear of prosecution."

An **anonymous chief legal officer** replied, "The government has been the most prolific user of people's private information, phone calls, etc. While this is done in the name of safety, it nonetheless diminishes everyone's privacy. I do not see things improving."

An **anonymous sociologist at the Social Media Research Foundation** wrote, "The need for security in IoT devices will lead toward oligopoly – only a few leading businesses will be able to provide a sufficient level of security. This will mean that the IoT world is one that leads toward monopoly."

An **anonymous** respondent commented, "The drive toward a more highly connected world is being motivated by corporate profits. Highly automated and connected devices allow these companies to maximize profits. However, the everyday person has little to no say in how certain types of networked devices (e.g., water meter) are deployed in their lives. The biggest threat currently is the loss of personal information. However, the future threats will be loss of life due to companies taking shortcuts in how they connect all these devices. While technologists can create protocols and network services that can help minimize threats, it will fall on governments to regulate how certain types of network connections (e.g., medical devices, power grid) are deployed/maintained."

Sam Punnett, research officer at TableRock Media, commented, "We are raising generations of people for whom the connected life is the norm. Increasing connectivity via IoT further complicates the environment and raises the potential for criminality and abuse. … I am not a network specialist but I have an appreciation for the world of IoT. If given the choice between a vision of the future made secure and safe I would be far more likely to ascribe to one put forward by the Electronic Frontier Foundation over one from any element of state surveillance and security."

Wendy M. Grossman, an independent writing and editing professional based in London, said, "Going forward, many will not have a choice about it. … If you can only have one device and one communications network, that's going to be a smartphone and a data plan, and if you can save money by consenting to let your refrigerator send the supermarket statistics on how and when you consume the groceries you buy, then you will. The problem is especially acute with respect to the technology underlying smart cities, because local authorities make operational decisions that don't require public consultations that have later impact on civil liberties and human rights. A great example is the auto-dimming streetlights being installed in a number of cities. Local residents, if asked, certainly support the goal of reducing energy use and cost; but they aren't consulted about the video and audio surveillance systems that form part of these systems. So: both of the statements we began with are true."

Axel Bruns, professor in the Digital Media Research Centre at Queensland University of Technology, wrote, "As with other trust issues, users may have significant concerns about data security in engaging with such networked objects – but in some cases their opportunities for opting out by choosing a non-networked device are likely to diminish rapidly. It is increasingly difficult to find new cars that do not feature back-to-base position tracking and networking as a default, for instance – so, as older models are disappearing from the marketplace, users will be forced to accept the embedding of such surveillance technologies into their cars (or find ways to hack them, potentially voiding the warranty)."

What do internet companies do with the data they collect? They do business with it. Of course. Nearly all internet systems, devices and services are created to generate a profit. A number of the participants in this canvassing pointed out that algorithms written to individualize people's experiences are narrowing choices for them in ways that are not to their advantage, not in the name of their personal convenience but in the name of generating corporate profits.

An **anonymous respondent** said, "I fear that data collected for marketing purposes will further narrow the range of products available to people, removing choice from the market and limiting options." Another **anonymous respondent** observed, "Perhaps that is the largest danger – networking is welcomed in as a convenience, but it actually proves to be a choice-killer."

An **anonymous respondent** observed, "There's an open question that's not quite about damage, safety or trust, but it will be fundamental. It's about how people think about and interact with these agents that collect and often act on information."

An **anonymous coordinator** said, “We already have these problems and people keep buying in. The greatest threats to me are the right to repair [IoT systems and devices] and the right to properly own your own purchased content.”

Another **anonymous respondent** warned, “Independence and privacy concerns will result in a fissure in society.”

An **anonymous respondent** urged, “There should be more ways to ensure that companies who make devices are ethically and civilly responsible to protect our data and that we can delete/erase/decide who gets it at every step. We don’t have that yet.”

An **anonymous digital manager** commented, “Privacy settings will be expanded if there are numbers indicating that people are disconnecting completely. Disconnecting in protest might be necessary in mass numbers to actually make this happen – it should be seen as a form of protest.”

D. Yvette Wohn, assistant professor at the New Jersey Institute of Technology, predicts that those with low socioeconomic status will have fewer options as the Internet of Things evolves. “The trend toward greater connectivity will take place among a majority of people (90%), but people who have very high income, are public figures or celebrities, or have very high adversity to technology will disconnect. The issue will not be about how we can make technology safer, but what is being done with the data that is collected. The government will come up with guidelines so that there will be different tiers of data that companies can use, based on the users’ preferences. People who are willing to have companies utilize their data more will receive stipends, creating a social imbalance where lower-income people will be more vulnerable to privacy relinquishment.”

Several other respondents said they expect that only the wealthiest people will find ways to disconnect and/or route around impositions on their civil liberties.

An **anonymous project manager** replied, “Connectivity will increase, and those able to pay more will be at the forefront of disconnecting or building isolated systems.”

An **anonymous IT director** wrote, “If people can afford to, they will disconnect and reduce the amount of digital ‘distraction’ or engagement in their lives. Paradoxically, it will be the most affluent who will be able to afford this ‘luxury.’”

Katharina Anna Zweig, a professor at Kaiserslautern University of Technology in Germany, commented, “As the connectivity promises more comfort, more safety, more savings, more almost anything (next to less privacy), most people will get more and more connected … I do not believe

that there will be a larger group of people totally disconnecting from the internet. It might become a privilege of the very rich, but they can only afford it because the people surrounding them and in their service are connected."

Luis Lach, president of the Sociedad Mexicana de Computación en la Educación, wrote, "People who decide to disconnect will be the ones with more information, but this will be an elite group of critical people. The market will win, no matter the consequences to our personal security and protection of personal data, and people will be connected. The more-concerning threat for the technological paradigm (positive or negative) is the evolution of global and local economies. Today, in the year 2016, … globalization is more of a risk to our lives than a social win. Fewer people are becoming richer in a stupid way, and a vast majority of the population is becoming poorer. We can see a map of world's migration, just to note that people from underdeveloped countries are migrating to the richest places (Europe and USA), and that is not because those geographies are lands of opportunity, it is because the countries they are coming from are being devastated."

An **anonymous respondent** replied, "We'll wind up being spied on not just by companies and governments, but third-rate hackers. Any individual who draws the anger of the online mob can look forward to having their basic life hacked. Ordinary devices have no business being connected to the internet. There will be a smaller but healthy market for security-conscious devices with limited connectivity. This might mean that only the wealthy and/or sophisticated have access to secure or unconnected options."

Dudley Irish, a software engineer, wrote, "This is a very complicated issue … but what I suspect will happen is that people will make changes that should lead to them being more disconnected, but in reality, they will be increasingly connected. I am a very knowledgeable technologist and *I* can't keep track of all the ways that my behavior is tracked. I consciously avoid being tracked and suspect that I am tracked much more than I would like. Meanwhile, most of the people I know can't be bothered to limit how much they are tracked because it just takes too much effort. And, it seems like every time I turn around I am reading about yet another privacy failure or technique for de-anonymizing data. This is a context in which regulation could help but is it very unlikely that any useful regulation will be done."

Alan Cain, a respondent who shared no additional identifying background, said IoT companies have the view that, "Your privacy belong[s] to us; we know when you are sleeping, we know when you're awake. We know if you've been naughty or nice, so be good for goodness' sake – a Shirley Temple future."

An **anonymous learning systems and analytics lead** wrote, “People will remain very skeptical but be left with fewer and fewer choices. Companies like Silent Circle cater to those who desire extreme measures around privacy, but it’s definitely a premium. This will continue to be the case. For example, it’s already economically silly to not accept the installation of driving-habit-tracking sensors. The iron cage of connected life will drive people to be more connected whether they want to or not – and many will not, or will at least have strong reservations.”

Christopher Wilkinson, a retired senior European Union official, commented, “Experience with algorithms is very mixed; [tech users] are naive. Privacy is not adequately protected. The algorithms create and retain personal information that is going to become intrusive over time.”

An **anonymous software architect** commented, “The surveillance state will only grow as the profit motive or ‘national security’ interests dictate. Most people will be unemployed and not be able to afford such conveniences or see them as time savers when they have too much time on their hands already (no jobs). This can come to no good end.”

Dan Caprio, co-founder of The Providence Group, commented, “We need to work together to protect privacy and security and enable innovation.”

Acknowledgments

This report is a collaborative effort based on the input and analysis of the following individuals.

Primary researchers

Lee Rainie, *Director, Internet, Science, and Technology Research*
Janna Anderson, *Director, Elon University's Imagining the Internet Center*

Research team

Aaron Smith, *Associate Director, Research*
Nick Hatley, *Research Assistant*
Kyley McGeeney, *Senior Research Methodologist*
Claudia Deane, *Vice President, Research*

Editorial and graphic design

Margaret Porteus, *Information Graphics Designer*
David Kent, *Copy Editor*

Communications and web publishing

Shannon Greenwood, *Associate Digital Producer*
Dana Page, *Senior Communications Manager*