IGF-USA 2011 Scenario: Government Prevails

Most of us assume that the ICT industry, media companies, and NGOs will continue to be the leading players on the Internet stage, with governments playing just a supporting role. This scenario describes an alternate future, where citizens and businesses worldwide turn to governments and inter-governmental organizations for protection and response to increasingly frequent and dangerous disasters.

MIND THE GAC

2011

In 2011, Internet governance was still dominated by a private sector that had invested over a trillion dollars to bring connectivity, content, and e-commerce to nearly 2 billion people worldwide. The private sector – including businesses and NGOs – were still doing most of the heavy lifting in setting IT standards, expanding the Internet's domain name system, and managing the transition to IPv6 addressing.

While governments pressed for a larger role in Internet governance, the private sector continued to drive Internet innovation, technology standards, and infrastructure investments. After some initial hesitation, governments were increasing their participation in multi-stakeholder fora such as ICANN and the Internet Governance Forum. From all appearances, it seemed in 2011 that multi-stakeholder models and consensus processes would shape the future of governance for the Internet, telecommunications technologies, and e-commerce.

However, mankind and mother nature combined to deliver a series of disasters and dangers that would overwhelm the plodding pace of any consensus-driven multi-stakeholder organization. Over time, this led most stakeholders to turn to governments for disaster responses and precautionary measures, many of which eroded the private sector’s role in Internet governance.

Looking at what transpired in 2011, perhaps we should have seen this coming. Several events that year sowed seeds of change in the role of governments in Internet oversight, ranging from the Arab Spring to the Stanley Cup to the Japanese Tsunami. Even video games and volcanic ash clouds contributed to the growth of government control over Internet resources.

2012

The 2011 protest movement known as the Arab Spring had wilted under the heat of government repression by early 2012. Regimes that survived the protests vowed never again to be outflanked by organizers’ use of online social media. These governments started by following digital footprints to track down dissidents. And they required all domestic telecom and Internet service providers to use deep packet inspection for tracking and logging all social media traffic.

The spring of 2011 saw another protest that drove greater government control over social media. After the Vancouver Canucks lost the final game in hockey’s Stanley Cup playoffs, a riot erupted in the city, causing fire and vandalism damage to vehicles and businesses. During the riots, citizens on the scene captured photos and videos of the mayhem, and posted them immediately to social media websites.

Within hours, hundreds of Vancouver social media users were “tagged” in videos and photos of vandalism and violence. Those who lost property in the riots used social media sites to organize vigilante justice squads against tagged individuals – even those whose only offense was being photographed while running away from a burning car or building.

The ensuing cycle of violence convinced Vancouver residents that vigilante justice was no substitute for police investigations and courtroom trials. The following year, Canada’s government passed new privacy laws prohibiting tagging of individuals in photos and videos on public websites. Other governments soon emulated Canada’s approach, effectively ending the popular practice of tagging friends on social media sites.

2013

The effects of two major disasters in 2011 drove trends in Internet governance in 2013. After the tsunami in Japan and river flooding in the US, online disaster relief scams captured headlines around the world. Criminals found they could take millions from well-meaning donors by hosting convincing websites with domain names like *TsunamiVictimFund.org* and *JoplinFloodRelief.com*. Media coverage of the fraud drove a decline in online global giving to disaster relief and other charitable efforts.

Then in 2013, ICANN launched nearly 200 new top-level domains for the Internet. Among them was .*Give* , whose sponsors promised to operate a trusted space for all charities, spending millions to educate individual and business donors about the new top-level domain.   Charities like the Red Cross and Red Crescent acquired their domain names in .*Give*, but most charities soon chafed under the .*Give* registry’s high fees and strict standards for relief operations and disclosure. By the end of the year, litigation and controversy drove the registry into bankruptcy, so ICANN invited an intergovernmental organization to take control of .*Give* domains and impose a new global regulatory regime for online giving.

2015

Back in 2011, Microsoft unveiled Kinect, a motion and image sensor with amazing range and accuracy. By 2015 these devices were under $50US, and governments began deploying the sensors in public buildings and on streetlamps. Banks and businesses installed these sensors, too, but only governments had access to a global database of facial images that could be matched in real-time. By the end of the decade, most governments could identify and track individuals who came within range of their sensors.   This proved helpful in finding missing persons and felons, but also enabled governments to identify and investigate dissidents appearing in street protests.

2016

After another series of volcanic eruptions in 2016, drifting ash clouds once again grounded air travel over much of Europe and Asia. Many businesses took another look at virtual video meetings as an alternative to air travel. And by 2016, new technologies and Internet bandwidth made virtual meetings almost as good as being there. As a result, more and more businesses scaled back on air travel in favor of virtual meetings and conferences.

By late in the decade, the drop in business travel was affecting airlines, hotels, and restaurants worldwide, while governments felt the loss of associated tax revenues. Under heavy lobbying from the travel and conference industries, governments began limiting the bandwidth available for real-time international video conferencing, citing the need to preserve bandwidth for domestic uses. These moves slowed the decline in business travel, but it never recovered to previous levels.

2017-2020

By the end of the decade, businesses and citizens around the world had grown weary of government budget cuts and austerity measures. At the same time, they grew anxious for comprehensive solutions to global problems. That sentiment found a new target amid growing concern over the levels of fraud, deception, and threatening content on the Internet.

Earlier in the decade, European courts convicted business executives for a video someone had posted to the company's website. This led to other convictions and private lawsuits over liability for user-generated postings and copyrighted material. In the US, 2017 saw the passage of controversial legislation regarding a black-list of websites that could no longer be served by ISPs, advertisers, payment services, or search engines.

By the end of the decade, most governments emulated the US and Australian approach and created black-lists of prohibited websites that included offensive content or copyright and TM violations. While this reduced some online threats, it was no help in stopping the virus attack of 2021, which emerged from within users' computers – not from Internet websites.

2021

For ten years, a mysterious computer virus had been quietly lurking in over a billion computers and mobile devices around the world. On April 1 of 2021, the 'Conficker' worm came to life – with a vengeance.   All at once, these infected computers contacted their organized criminal controllers to upload credit card and identity data they had been collecting for a decade. Credit card fraud was rampant for months, as users around the world canceled accounts and watched for new accounts opened with their stolen credentials.

Conficker became the disaster that finally drove consumers and industry to demand that governments monitor all network traffic and scan users' computers for the presence of malware. It also drove banks and businesses to demand that governments take unprecedented steps to battle credit card fraud, lobbying for government-issued biometric authentication credentials for all digital citizens.

While these user authentication services were originally designed to serve e-commerce, they were also embraced by online services looking to reduce legal exposure for user-generated content and copyright infringement. Social networks, blog sites, and video services soon required authenticated identities before publishing content – bringing an end to whatever anonymity remained on the Internet.

2022

The year 2022 brought the most devastating tropical storms in recorded history. Coastal flooding and storm damage in equatorial regions caused tens of thousands of people to go missing, often for several days. Dramatic rescues captured media attention, and many of those survivors credited GPS transponders that were integrated with the latest high-end smartphones. By the end of the year, many governments passed popular mandates to require precise location-tracking technologies in all mobile devices—without the option to disable. Proponents cited the obvious benefits for search-and-rescue and 911 responders, swamping those who complained about this further erosion of personal privacy.

2023

The unprecedented storms of 2022 were the tipping point that motivated governments around the globe to take collective action to stem global warming.   In 2023, global governments signed the EarthSave Treaty, which included enforcement mechanisms to require reductions in greenhouse gas emissions. The treaty required monitoring of all significant point sources of carbon dioxide and thermal pollution, creating instant demand for portable infrared sensors and gas chromatographs. Within a year, these sensors were available on smartphones, empowering a global network of “EarthSave Snitches” to capture emissions images of vehicles and factories and instantly send them to environmental authorities – along with GPS location and identity of the offender.

2024-2025

Since 2020, governments around the world were acquiring unprecedented powers to regulate financial markets, energy and food supplies, and just about anything that could be causing global warming. These new powers came in small increments and varied widely among nations, but a common theme was the growing reliance on virtual government services enabled by extensive surveillance and monitoring tools.

Local and state governments fully embraced a services model that was almost entirely online and available any place and at any time. This model was also highly interconnected among all levels of government, which proved invaluable when coordinating regional responses to disasters and to shortages of food, fuel, or water. Based on these successes, many local governments sought to merge their functions with other local and regional authorities. The trend for consolidation made it apparent that local governments would soon become relics of history.

This trend of connection and consolidation extended far up the governmental chain of command. Most national governments – including the US – were keen to build on the success of multi-national cooperation to fight terrorism and respond to disasters. And multi-governmental organizations like the United Nations took every opportunity to coordinate and consolidate power under various mandates for global solutions.

At many points in the process, there were public protests and legal challenges from advocates of free expression and groups suspicious of an intrusive, 'big brother' government. But the tide of public opinion and industry enthusiasm carried the day.   By 2025, governments and law enforcement had become deeply embedded in all aspects of Internet communications, content, and e-commerce.