THE IOT REVOLUTION AND OUR DIGITAL SECURITY:

Principles for IoT Security

U.S. CHAMBER OF COMMERCE

Wiley Rein LLP

U.S. CHAMBER OF COMMERCE

The U.S. Chamber of Commerce is the world's largest business federation representing the interests of more than 3 million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations.

Wiley Rein LLP

Based in Washington, D.C., Wiley Rein LLP operates at the crossroads of law, politics, business, and technological innovation. The firm represents a wide range of global clients in complex, high-stakes litigation as well as regulatory and transactional matters. It helps bring products and services to market globally. Wiley Rein has 250 attorneys and public policy advisors, many of whom have held high-level positions in the White House, on Capitol Hill, and in federal agencies. Our lawyers offer unique insight into the fast-changing regulatory, business, and economic climate in which our clients operate, and help them find creative solutions to the legal and geopolitical issues that impact their business.

THE IOT REVOLUTION AND OUR DIGITAL SECURITY

Principles for IoT Security

TABLE OF CONTENTS

FOREWORD

Today the Internet of Things (IoT) is poised to revolutionize the future in advanced and developing economies. The coming IoT revolution is set to unleash enormous business and consumer gains. But the explosion in the number of internet-connected devices presents a significant increase in the attack surface and methods for malicious actors. The recent surge of cyberattacks continues to increase in scale, sophistication, and frequency, and they will pose a threat to the privacy and security of public and private institutions and consumers.

Facing such threats, companies view privacy and security as crucial and an essential part of risk management. Businesses are leading global efforts to strengthen the security of their information systems and products, mitigate system vulnerabilities, and improve public-private cooperation to deflect and defeat these threats.

This paper provides an overview of the growth and innovation in the IoT ecosystem, followed by a discussion of the challenges to securing the IoT and the significant ongoing public-private work to enhance security. It concludes with recommendations that can help policymakers and industry experts collaborate on reducing barriers to innovation and co-creating global frameworks to improve security.

The principles for IoT security are intended to be relevant and timely for anyone responsible for developing policies promoting innovation and global collaboration. I hope you will find this report useful in helping to bring about a more secure digital future.

Ann M. Beauchesne
Senior Vice President
National Security and
Emergency Preparedness
U.S. Chamber of Commerce

Megan Brown
Partner
Wiley Rein LLP

Sean Heather
Vice President
Center for Global
Regulatory Cooperation
U.S. Chamber of Commerce

EXECUTIVE SUMMARY

Future growth predictions for the IoT are staggering. At this inflection point, regulatory philosophy will impact the pace and path of innovation. With a truly global market for the IoT, national boundaries and policy differences threaten to create barriers and walled gardens and distort markets. Governments should support international standards work that harmonizes varied approaches to regulating technology.

Governments are in a difficult position given the complexity and fast changing cyber threat landscape and traditional regulatory responses are inadequate to keep pace with the evolution and economic growth potential of the IoT.

Consumers may not be prepared for their roles in our digital future, in which individual actions can affect communities and enterprises around the world. Basic cyber hygiene education should be prioritized by governments, businesses, and consumers.

Similarly, increased attention is being paid to hardening endpoint security. Here, manufacturers and vendors are leveraging existing industry-developed best practices. They should be encouraged and incentivized to pursue security by design.

Recent cyberattacks like WannaCry, Petya, and Mirai illustrate why a combination of end user education and endpoint security is important. WannaCry and Petya victims used unsupported and unpatched versions of legacy operating systems, which is a lesson in the importance of upgrading and patching devices. Likewise, the Mirai botnet depended on wide-spread use of a common set of credentials, which speaks to use of hardcoded passwords. Governments should proactively collaborate with industry to identify and facilitate voluntary use of best practices.

Given how diffuse and ubiquitous the IoT is, the global effort to enhance security, privacy, and trust requires input from public and private stakeholders. Governments should establish international multi-stakeholder forums for discussion and education about security and privacy regulations, and trust enhancing certification and labeling frameworks.

The IoT is incredibly complex and there is no one-size-fits-all solution to cybersecurity. But the business community looks forward to working with governments to collaboratively create policies that enhance privacy, security, and trust in the IoT based on global, voluntary, consensus, and industry-driven standards.

TEN KEY PRINCIPLES FOR IoT SECURITY

1. When it comes to security, attempts to regulate today will become outdated tomorrow. Flexible approaches to collaboration and cooperation to combat shared threats have significant advantages over national regulation which serves to fragment the global economy and lags behind technological innovation.

2. Any approach to IoT security should be data-driven, based on empirical evidence of a specific harm, and be adaptable both overtime and cross-border.

3. Security demands should never be used as industrial policy to advance protectionism or favor national economic interests.

4. National boundaries need not become arbitrary obstacles to the movement of devices or data, or to the offering of IoT-related services.

5. Global standards work is the best way to promote common approaches and technology solutions. Such standards should be open, transparent, and technology-neutral.

6. Any government IoT strategy should promote technical compatibility and interoperability to the maximum extent possible.

7. Everybody is vulnerable, cyber threats must be met with global information sharing and collaboration to improve and safeguard the IoT ecosystem.

8. End users need to be educated about their roles and responsibilities in this digital age.

9. Manufacturers and vendors should be encouraged to routinely evaluate and improve endpoint security.

10. The international community must collectively condemn criminal activities that infect and exploit the openness and connectivity of the internet and our digital future. Governments must work together to shut down illegal activities and bring bad actors to justice.

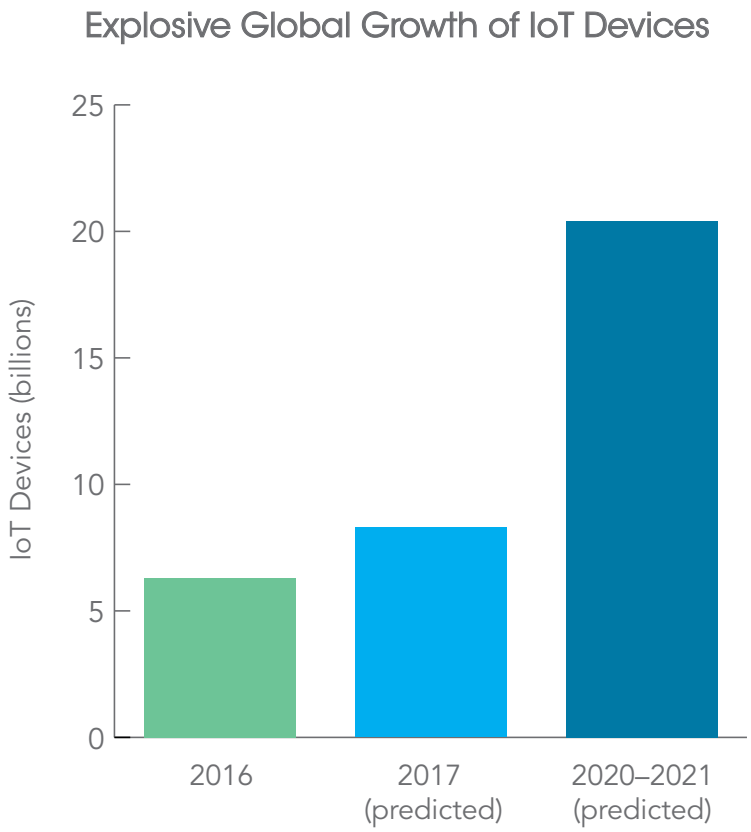
I. THE INTERNET OF THINGS—AN IMMINENT REVOLUTION

WHAT IS THE IoT?

The IoT ecosystem is diverse in potential use cases, users, and contexts. **The IoT is made up of things** (e.g., tags, sensors, and devices) that connect through a network—often to the cloud—from which data can be collected, shared, and analyzed to create value. Examples of things include appliances (from refrigerators[1] to toasters[2]), personal hygiene products (like hair brushes[3] and toothbrushes[4]), medical devices, cars, smart phones, smart roads, smart electric meters, and machinery, to name just a few. **The IoT is also made up of data.** Connected "things" generate data, which are shared and analyzed. **The IoT also consists of the network and services that enable the communications:** wireless, satellite, and fiber communications systems that are critical to moving data between the things. Finally, **the IoT is made up of people**—consumers, enterprises, organizations, and other end users who interact with or depend on the **things, data, networks, and services**. This complexity is why some call the IoT the Internet of Everything.

Credit: U.S. Chamber of Commerce

IoT growth is poised to explode. According to a recent international study, 57% of companies have adopted IoT technology, with 85% expected to do so by 2019.[5] Consumers, however, and not companies, now are the largest set of IoT users, though that may change. In 2016, 3.9 billion consumer units were connected to the IoT.[6] That group together with business accounted for a total of 6.3 billion IoT devices in 2016.[7] For 2017, the number is expected to be 8.3 billion.[8] **Future predictions are staggering.** Every hour, a million new IoT connections are made.[9] Ericsson estimates that between 2015 and 2021, the number of IoT-connected devices will grow by 23% each year.[10] Information technology research company Gartner predicts 20.4 billion IoT devices by 2020.[11] Ericsson projects that of the estimated 28 billion total devices that will be connected by 2021, close to 16 billion will be IoT devices.[12] Other firms estimate even more IoT growth—with one assessment indicating that there will be 46 billion connected devices, sensors, and actuators by 2021.[13] The European Union (EU) is poised to experience this IoT expansion along with the rest of the world. In 2020, it is estimated that there will be 6 billion IoT connections in the EU. This number is up from just 1.8 million connections in 2013.[14] IoT growth has been and will continue to be explosive.



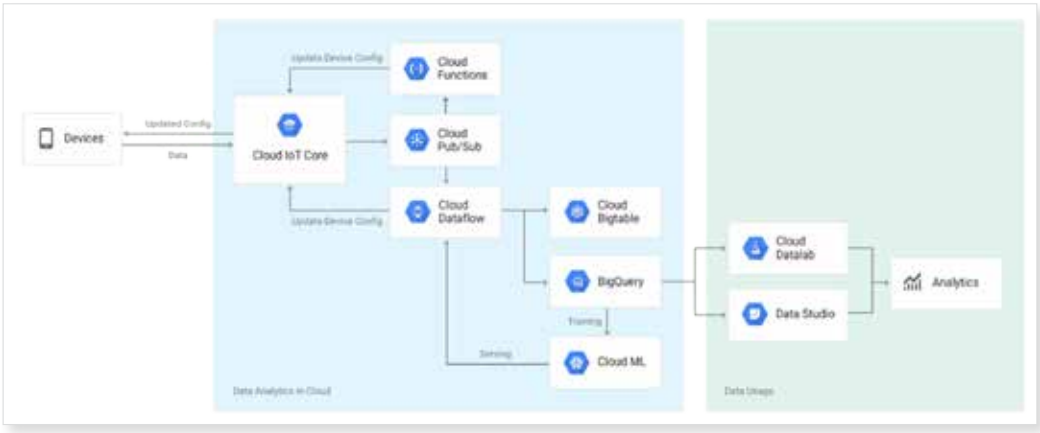
THE IOT REVOLUTION AND OUR DIGITAL SECURITY

Principles for IoT Security

Distinctions important for policymakers to understand are likely to emerge as the IoT matures. One distinction is a ***consumer versus an industrial IoT***. A consumer IoT connects devices like smart TVs, appliances, gaming consoles, wearables, and smart phones; an industrial IoT provides connectivity in industrial environments via such devices as factory equipment, environmental sensors, retail systems, security cameras, medical appliances, and digital signs. While these categories may overlap as enterprise settings utilize products that are available to consumers, these distinctions may provide a proxy for oversight and regulatory efforts. Enterprise and industrial settings are likely to need little government oversight. There is more likely to be parity in the sophistication and bargaining power of the parties in industrial and enterprise settings. Large enterprises managing fleets of sensors and equipment will be quite capable of protecting their networks and data using service level agreements, device requirements, enterprise IoT management tools, and insuring themselves against disruptions.

Another distinction is an ***unmanaged versus a managed IoT***. An unmanaged IoT refers to individual devices that are connected and managed by individual end users. A managed IoT refers to services and devices that are managed by a third-party provider or a cloud-based IoT management platform. Managed service markets may include cloud security and network, data, and device management tools that focus on enterprise and home settings.

A managed services approach could address many of the security concerns surrounding the IoT. Large, experienced internet, cloud, and hosting companies know how to offer large-scale services and support, which could make it easier for policymakers to focus on the most troubling use cases and security risks. A managed approach also creates an intermediate layer that allows for more control. The policy implications for unmanaged IoT are different. Non-managed IoT could mean a lack of device interoperability, poor quality, and unprepared networks, which may make it harder to implement IoT security.



Credit: Google

User needs—as well as expected network, service, and device capabilities—are likely to differ across these settings. Different policy considerations will likely emerge for each type of IoT. In general, business and consumer uses of IoT must further develop before policymakers are well informed to assess any potential policy response.

IoT SUPPLY CHAINS, DISTRIBUTION CHANNELS, NETWORK SUPPORT, AND PHYSICAL PRESENCE ARE INHERENTLY GLOBAL.

IoT supply chains will depend on global mobile and internet networks, software developers and vendors scattered around the world, hardware manufacturers from various countries, and value-added integrators in myriad jurisdictions.

IoT devices can be everywhere: examples include tracking devices on shipping containers crossing the ocean and sensors adjusting agricultural water use, as well as consumer products available for sale globally by multinational companies. The global nature of the IoT supply chain and the vast differences in law and policy across countries introduces security risks and widens the threat landscape. No amount of security in any network can fully address these global threats. Country- or region-specific device requirements ignore the vast global supply chain for IoT, with software, OS, application, hardware, and service providers located around the globe, including developed and developing countries. The task of securing the IoT must cross geographic boundaries because the IoT supply chain is globally dispersed.

Credit: Screens Magazine

THE IoT CAN REVOLUTIONIZE THE FUTURE IN ADVANCED AND DEVELOPING ECONOMIES.

JAPAN: SOCIETY 5.0

Japan is focused on "shaping a world-leading 'super smart society' (Society 5.0) that address both economic development and societal challenges."[22] IoT is at the heart of Japan's Society 5.0–"In order to realize a super smart society, it is necessary to connect various 'things' via a network, create highly advanced systems out of these things, and integrate several diverse systems so that they can coordinate and collaborate with each other. This integration allows for a wide variety of data to be collected, analyzed, and applied across all the coordinating and collaborating systems in order to continuously produce new values and services."[23] The Japanese government has recognized that "it is not realistic to believe that a framework capable of enabling the coordination and collaboration of all kinds of systems could be constructed right away," and that realizing a "super smart society" will require collaboration between industry, academia, and the government, including relevant ministries and agencies.[24]

The IoT is part of what some have called the Fourth Industrial Revolution.[15] This revolution, which "combine[s] the physical, digital and biological worlds,"[16] will "transform the way we live and do business."[17] The benefits of the IoT will not be restricted to advanced economies; studies predict incredible benefits, including "leapfrog gains,"[18] particularly in agricultural, industrial, and environmental use cases across the developing world. IoT data will allow us to extract insights, create new opportunities, and solve problems in ways that have not been possible until now.[19] From addressing greenhouse gas emissions to combatting world hunger, "smart and connected systems can tackle these problems."[20] The benefits of the IoT will be substantial and revolutionary.

Case Study: Smart Cities

Intel, Imperial College, and University College London have created the Intel Collaborative Research Institute for Sustainable & Connected Cities, a research program aimed at transforming IoT initiatives into real-world urban applications. It "seeks to bring an interdisciplinary approach to enable a Smart City to be more connected and sustainable by combining methods from computer science, the social sciences, interaction design, and architecture in order to improve how cities are managed and maintained and enhance citizen well-being."[21]

Benefits to consumers will be immense. The IoT is changing the way people live. From devices and services that make life more convenient (e.g., applications that adjust thermostats or preheat ovens) to devices that save lives (e.g., wireless infusion pumps[25] and asthma management kits[26]), consumer IoT devices allow for "virtually any and every thing [to] be connected to the Internet."[27] Consumers will reap benefits like improved customer experiences and personalization,[28] improved quality of life, and enhanced safety, among others.

Case Study: Public Health Sector

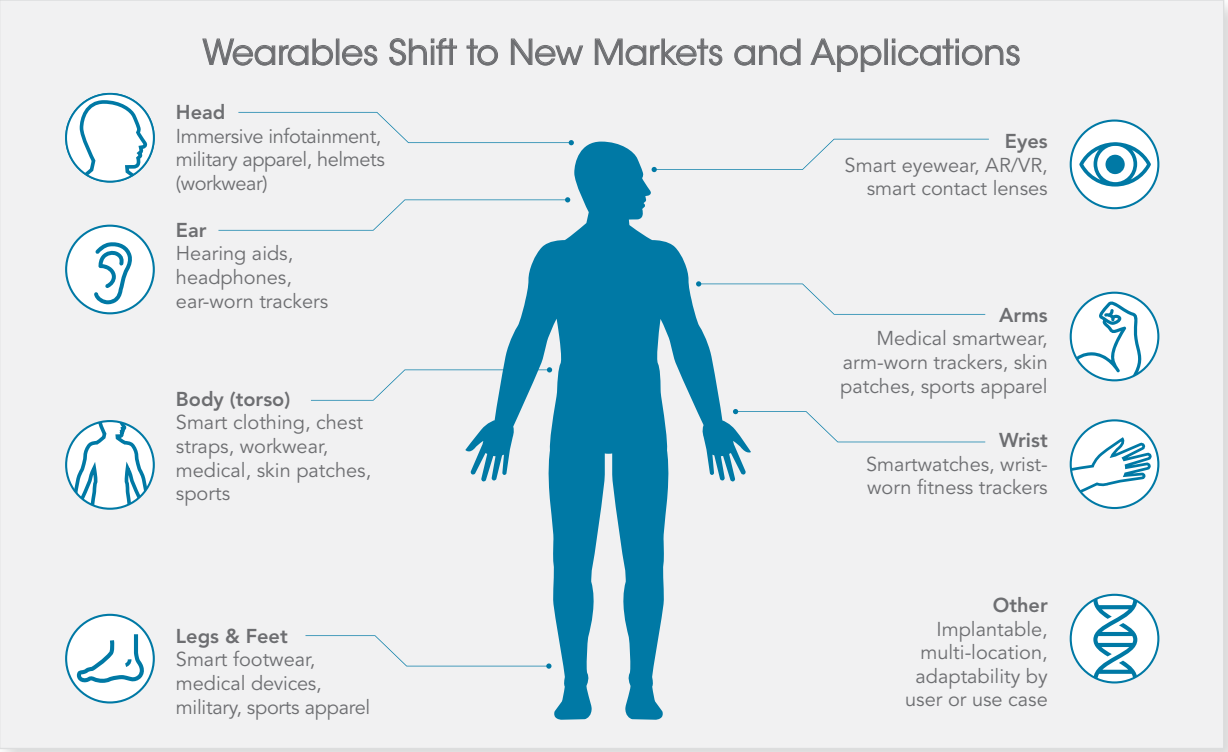
IoT is promising for public health, with important impacts in developing countries.

For example, "IoT technologies are also being used to address immediate challenges in humanitarian response, such as the Ebola outbreak in West Africa. The United States Agency for International Development (USAID) has supported and employed IoT solutions via connected wearable technologies. Sensor Technology and Analytics to Monitor, Predict, and Protect Ebola Patients (or STAMP2 for short) has been tested on Ebola patients in the United States and is being scaled up to meet the needs of government agencies such as USAID for its Ebola treatment strategy in Liberia."[29]

IoT has helped "monitor the 'cold chain' delivery of vaccines, particularly to remote and rural areas."[30] Vaccines must be kept at particular temperatures, and manual monitoring refrigerators across the developing world has been challenging. With IoT sensors in refrigerators, data about problems can be sent to local and district coordinators, and aggregated at the national level to "determine how to allocate limited maintenance and equipment resources, and where vaccine doses can be safely delivered (i.e. to ensure a batch of vaccines is not dispatched to a broken refrigerator)."[31]

Case Study: Wearables

Wearables are connected devices designed to be worn by a person. Ranging from smart eyewear and smart contact lenses to fitness trackers and smart clothing, the demand for wearables has exploded as these devices offer significant value to consumers. One prediction indicates that global wearable shipments will reach 213.6 million units by 2020.[32]



Credit: IDTechEx

Benefits for business will be substantial. The IoT in the workplace improves effectiveness, enhances productivity, boosts innovation, expands visibility across organizations, saves money, and increases profitability.[33] Seventy-two percent of enterprise organizations globally "have introduced IoT devices and sensors into the workplace—from air conditioning and lighting systems … to personal mobile devices."[34] Businesses also use the IoT to track important assets,[35] reduce operation risks,[36] and address downtime.[37] The use cases are variable and diverse, with new uses constantly being innovated.

The IoT will help our environment. Smart devices can yield environmental benefits as well. For example, IoT capabilities allow for businesses and homes to more efficiently manage utility use, which ultimately reduces energy and water consumption.[38]

Case Study: Sustainability

Telefónica UK is rolling out 53 million smart meters across the U.K. by 2020. The U.K. Department of Energy and Climate Change estimates that the program will yield net benefits of £6.7 billion in reduced energy consumption and more efficient management and deployment of electricity services across the country.[39]

Benefits for economic growth will be substantial. McKinsey estimates that the "IoT has the potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025. At the top end, that level of value—including the consumer surplus—would be equivalent to about 11 percent of the world economy."[40] Cisco estimates that the potential value of the IoT is even higher: $14 trillion.[41] The U.S. Chamber of Commerce estimates, "[t]he Internet of Things could add as much as $15 trillion to global GDP over the next twenty years."[42]

The IoT will boost new jobs. Studies have shown that advancements in technology and the rise of machines creates jobs.[43] In general, "while advances in technology may displace certain types of work, over a long-term horizon technology has been a net creator of jobs. … The advent of IoT is no different, and much like the industrial and technological revolutions that preceded it, we'll find that instead of fearing for our jobs, we should embrace the fact that IoT will take the mundane activities out of our work lives and offer new, unique opportunities to evolve and expand our skill sets."[44]

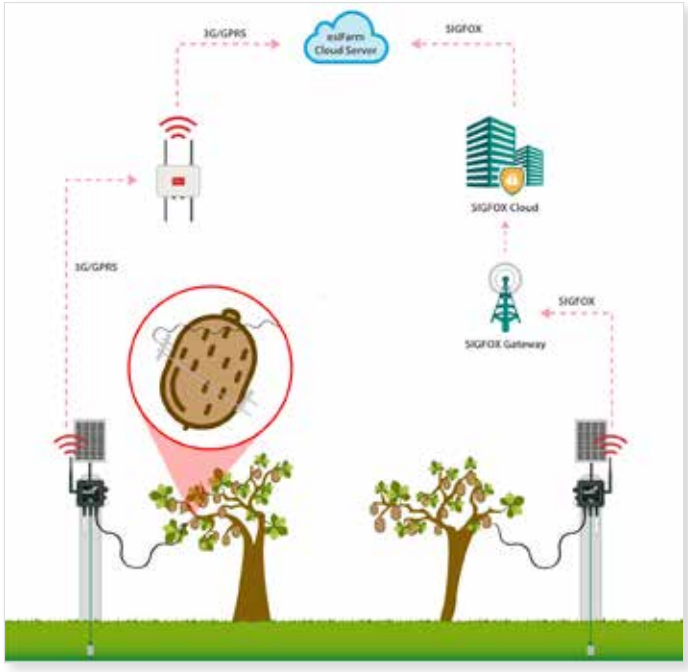
SOUTH KOREA: MASTER PLAN FOR BUILDING THE IOT

Recognizing that the forecasted growth in the global IoT market is expected to "bring[] diverse innovations and creat[e] business opportunities," and setting a goal to "stand as a leader of the global market with its top-class ICT infrastructure and manufacturing capacities," Korea's Ministry of Science, ICT and Future Planning released a *Master Plan for Building the Internet of Things (IoT) That Leads to the Hyper-Connected, Digital Revolution*.[45] In it, Korea sets forth several strategies for IoT development, including increased collaboration between the "entire government (ministries and local governments) and the private sector (businesses)."[46]

The IoT will aid in agriculture and food security. Precision farming and smart agriculture will help meet growing demand for food. The United Nations predicts that "[t]he world will need to produce 70% more food in 2050 than it did in 2006 in order to feed the growing population."[47] Farming efficiencies will be critical to meet this need. The U.S. is both the country that produces the most crop yield per acre of farmland and the country that leads in the deployment of IoT smart agriculture.[48] These benefits can be realized across the globe as countries promote better agricultural practices and innovation.

Case Study: Agriculture

Famosa, an Italian technology company, offers technology-based solutions for crop monitoring and management. Famosa has developed a smart solution to meet the irrigation needs of Italian kiwi farmers, allowing "[f]armers [to] get valuable information to schedule irrigation timing to avoid stress conditions, which is fundamental on kiwi plants." Italy is second only to China in kiwi production. Smart technology, like the smart irrigation system, will help to improve farming processes (ultimately resulting in more products brought to market and fewer products that are lost) and lessen the daily burdens of farming.[49]



Credit: Libelium

The IoT will boost research. IoT is enabling a "revolution in research across every sector of the economy to analyze new information. … Research in medicine, science, and commerce will employ new data analytics on a scale never before possible."[50]

NEXT GENERATION WIRELESS AND WIRELINE TECHNOLOGIES, INCLUDING 5G NETWORKS, WILL PAVE THE WAY FOR INNOVATIVE COMMUNICATION PATHS AND TECHNOLOGY.

The future of global connectivity will be driven by the availability and reliability of next-generation wireline and wireless networks, including Fifth Generation or 5G licensed and unlicensed wireless technologies. This next generation of wireless is being engineered to address capacity and speed needs that will be key to supporting consumer and business needs for high-speed, quality data and reliable connectivity in order to drive innovative technology solutions.

Capacity: IoT growth is a major driver of expanding spectrum demand. As more things are connected to the internet, utilizing licensed and unlicensed bands, the need to use spectrum effectively and efficiently will become even more important.[51] 5G's robust capacity, reliant on a mix of licensed and unlicensed spectrum bands and a variety of radio access technologies as well as high-speed wireline backhaul, will better accommodate dense usage patterns and data-rich applications associated with the IoT.[52] Next generation networks, including 5G, will offer significant capacity gains.[53] "5G will be able to support massive connection density, possibly on the order of 100 times greater than 4G LTE (Long-Term Evolution),"[54] while next-generation Wi-Fi networks will support up to a four-fold increase in capacity over the current generation. This makes the array of smart devices and other things in the IoT ecosystem possible.

Speed: Additionally, next-generation licensed and unlicensed wireless networks will power the IoT by dramatically increasing network speeds. 5G promises a ubiquitous, very high-speed wireless network.[55] 4G networks offer consumer speeds of 10-20 Mb/s, on average. Licensed wireless and gigabit Wi-Fi networks will be more than 10 times faster, potentially over 1,000 Mb/s. This type of speed will allow consumers and businesses to take advantage of IoT functions and services without delay and without decreased quality.

Latency: Finally, next-generation networks will offer lower latency, which will allow for technologies to provide consumers and businesses with real-time solutions, such as live traffic updates. This will have positive impacts for infrastructure, citizen

convenience, public transportation, and public safety, just to name a few benefits in one IoT area—smart cities. Reduced latency is also a critical feature of 5G network intended to support smart cars. It is predicted that 5G latency rates will be five to 10 times lower than 4G LTE latency rates.

IoT SECURITY IS A GLOBAL CHALLENGE REQUIRING FLEXIBILITY AND SUPRANATIONAL COLLABORATION.

THE COMING EXPLOSION IN IoT DEVICES PRESENTS AN INCREASE IN ATTACK SURFACES AND METHODS.

Botnets and other automated distributed attacks are a danger to the IoT and the consumers and businesses that use it. The exponential increase in connected devices, some with hardcoded credentials, presents an enormous attack surface. Botnets were originally created for useful purposes but have been exploited to wreak havoc and do harm. Global companies, infrastructure, and governments have been victim to recent cyberattacks.

Experts agree that an increase in endpoint prevention is just as important as ongoing mitigation efforts at the network level in responding to distributed and automated attacks like botnets.[56] In the United States, the Communications Sector Coordinating Council, a body comprised of five segments including broadcast, cable, wireless, wireline, and satellite and represents over 40 organizations, identified ongoing progress and needed improvements in basic device security, such as "ensur[ing] all end-points including IoT devices adhere to industry developed security standards," devices run up-to-date software, and networks that use IoT employ filtering and segmentation.[57]

RECENT CYBER INCIDENTS

Petya. In June 2017, a strain of ransomware called Petya spread rapidly. The government of Ukraine was hardest hit, but Petya also spread through large firms including advertiser WPP, food company Mondelez, and Danish shipping firm Maersk.

WannaCry. In May 2017, another strain of ransomware, WannaCry, infected hundreds of thousands of targets, including public utilities and large corporations. WannaCry temporarily crippled National Health Service hospitals and facilities in the United Kingdom.

Mirai. The Mirai botnet used devices in over 150 countries for a massive distributed denial of service attack, including against a French web-hosting provider and against domain name system provider Dyn in October 2016.

THE PRIVATE SECTOR IS NOT STANDING STILL IN THE FACE OF INCREASED RISK FROM THE IoT.

A Gartner report estimated that "[w]orldwide spending on [IoT] security will reach $348 million in 2016, a 23.7% increase from 2015 spending of $281.5 million. Spending on IoT security is expected to reach $547 million in 2018."[58] By 2020, Gartner predicts that over half of all IoT implementations will use some form of cloud-based security service.

Solutions are being developed and offered globally. As Symantec explains, security architectures are being refined to support comprehensive security because "IoT systems are often highly complex, requiring end-to-end security solutions that span cloud and connectivity layers, and support resource-constrained IoT devices that often aren't powerful enough to support traditional security solutions."[59] Increased attention is being paid to authentication and encryption. All of these things will improve security in the IoT, and it is vital that these innovations have a global reach.

TECHNOLOGY ALONE CANNOT ADDRESS IoT SECURITY; COLLABORATION IS CRITICAL.

Innovations in technology alone cannot solve the IoT security challenge. As the European Union Agency for Network and Information Security (ENISA) explains about botnets, "[g]lobal cooperation is an indispensable condition for the successful investigation of botnets. … In particular, the heterogeneity of legal situations in different countries suggests a need for the harmonisation of related laws."[60] As explained below, harmonization and collaboration will be key to IoT security.

ENISA is modeling that cooperation by supporting European Energy-Information Sharing & Analysis Centre and joint response efforts in Computer Emergency Readiness Teams and related bodies.[61] The more success that companies and governments have in these settings, the better the entire ecosystem will be at sharing and working against our common enemy: those who seek to exploit connectivity in order to do harm to others.

Case Study: Vehicle Cybersecurity Program

UL, a global independent safety science company, recently established a vehicle cybersecurity program and laboratory in Silicon Valley. The vehicle cybersecurity program aims to support manufacturing efforts to make vehicles more resilient to cybersecurity exploitation, by advancing secure automotive technology through ongoing research, testing, and repeatable methodologies.

ROBUST IoT SECURITY STANDARDS ARE BEING DEVELOPED AND DEPLOYED.

INDUSTRY IS LEADING THE GLOBAL DEVELOPMENT OF STANDARDS AND BEST PRACTICES.

Numerous global entities are engaged in global IoT security efforts.

The European Telecommunications Standards Institute (ETSI) is heavily involved in developing voluntary standards for IoT security, including security for smart appliances, smart cities, smart metering and grids, eHealth, intelligent transport systems, and wireless industrial automation.[62]

The Groupe Spéciale Mobile Association (GSM Association, or GSMA), a trade body representing mobile operators worldwide, is a prime example of industry leadership. The GSMA has issued a four-document set of recommendations for enhancing security at every stage of the IoT value chain.[63] The first document provides an overview of existing security challenges and available solutions for IoT service providers, device manufacturers, developers, and network operators for enhancing security.[64] The second document examines security in the service ecosystem, offering recommendations for mitigating threats to IoT servers and databases, network elements, and other technologies that support internal components of IoT products or services.[65] The third document evaluates security from the device endpoint perspective—everything from consumer wearables to automotive telematics and unmanned aerial systems.[66] The final document offers guidance for network operators serving IoT service providers.[67] In addition to developing industry-driven guidelines and best practices, the GSMA prepared a voluntary IoT security assessment process to help IoT companies identify and mitigate potential security vulnerabilities.[68] The organization has also published guidance on IoT authentication using SIM cards.[69]

The IoT Security Foundation (IoTSF) coordinates an international focus on security across the IoT application space. It is a collaborative, vendor-neutral, international initiative aspiring to be the expert resource for sharing knowledge, best practice, and advice. It has an on-going programme designed to propagate good security practice, increase adopter knowledge and raise user confidence.

The UL Cyber Assurance Program (CAP) offers a suite of best practices and solutions that assess software vulnerabilities and weaknesses, reduce exploitation, address known malware, review security controls, and enhance security awareness. The program offers the ability to evaluate both the security of network-connectable products and systems as well as processes for developing and maintaining products and systems with a security focus. The CAP and the 2900 series standards provide a reliable tools and set of requirements to ensure that manufacturers of internet-connected devices meet certain security criteria.

See **Appendix A** for a listing of select standards organizations developing recommendations to facilitate IoT security.

COMPANIES ARE IMPLEMENTING BEST PRACTICES TO ENHANCE SECURITY IN NETWORKS AND DEVICES.

Global manufacturers, network operators, and technology companies are working to advance the security of devices and networks. Although efforts may be uneven globally, best practices are emerging and guiding private-sector innovation. Global network operators are moving communications security forward. For example, telecom operator Telefónica, with industry partners and the Port Authority of Seville, Spain, is using the GSMA IoT security guidelines to improve its planned "Tecnoport 2025" project—an IoT system that will facilitate tracking and control of containers passing through the port as well as optimize rail and river traffic.[70] "In line with the GSMA IoT security guidelines, Tecnoport 2025 uses a combination of virtual private networks (VPNs), private access point names (APNs), multiple-factor authentication mechanisms and other measures to keep the new IoT solutions secure."[71]

The emerging consensus is that endpoint security will be paramount. Global supply chains confirm that device security is a major challenge—and one that is not solvable by one country or region. As society goes through the growing pains of the early IoT, we are identifying best practices, which can include endpoint hardening, such as port locks and camera covers. But security boils down to "a layered approach that requires attackers to circumvent a variety of obstacles designed to protect the device and its data from illicit access and use."[72] It can also include strong boot-level passwords or requiring the device to boot from local storage. Consensus is emerging about the need to consider future patching and upgrades as well as lifecycle management, future obsolescence, and related issues. There is no single solution for these issues across the diversity of IoT products, services, and deployments, but best practices will evolve.

AT THIS INFLECTION POINT, REGULATORY PHILOSOPHY WILL IMPACT THE PACE AND PATH OF INNOVATION IN THE IoT.

For the past few decades, the dominant narrative in global policy debates was largely built on the twin pillars of promoting competition and increasing liberalization across industries, including in the telecoms and internet sectors. This paradigm was deregulatory in nature and saw protectionist policy as inherently undesirable and the free flow of information and capital as values to be promoted. This was critically important for the growth and success of the internet.

A different outlook is developing in some parts of the world. There is active reconsideration of the wisdom of liberalization and competition-based policies. This is being expressed in many ways, including increasingly fragmented approaches to privacy, security, and domestic consumer protection regulation; protection of domestic industries and national champions; and an increased role of national government and intergovernmental organizations in previously unregulated or loosely regulated markets. If this trend takes hold, innovation and advantages of global scale and scope will be undercut by increasing rules and regulations, which foster uncertainty, and compliance obligations, which may have little benefit.

With a truly global market for the IoT, national borders and policy differences should not act as barriers. The IoT needs to be able to operate and move across national boundaries. Divergent regulatory approaches may challenge interoperability as well as the scale needed to realize the full potential of the IoT.

Policy responses on the rise that represent challenges often embody:

- Imposing unnecessary and inefficient compliance costs.
- Restricting data moving across jurisdictions
- Diverging security regulations that distort markets and require the creation of walled gardens or regional IoT sectors.

Now is the time to be vigilant in preventing any regulatory barriers that could slow the promise of the IoT.

SMART DEVICES REQUIRE SMART REGULATION.

NATIONS SHOULD DEVELOP UNIFIED IoT STRATEGIES INFORMED BY EXPERIENCE, DATA, AND STAKEHOLDER INPUT.

Because the IoT market is still developing, it warrants careful study and thoughtful national strategies. Ultimately, a regulatory response, in part, may be helpful, but only where it meets a demonstrated need and not already addressed by existing regulation.

In aspiration terms, U.S. President Barack Obama described U.S. regulatory practice in the following manner:

"Our regulatory system must protect public health, welfare, safety, and our environment while promoting economic growth, innovation, competitiveness, and job creation. It must be based on the best available science. It must allow for public participation and an open exchange of ideas. It must promote predictability and reduce uncertainty. It must identify and use the best, most innovative, and least burdensome tools for achieving regulatory ends. It must take into account benefits and costs, both quantitative and qualitative."[73]

Our regulatory system "must be based on the best available science," and "[i]t must identify and use the best, most innovative, and least burdensome tools for achieving regulatory ends."

President Obama

And President Donald Trump, in an Executive Order on strengthening the cybersecurity of federal networks and critical infrastructure, said "[t]o ensure that the internet remains valuable for future generations, it is the policy of the Executive Branch to promote an open, interoperable, reliable, and secure Internet that fosters efficiency, innovation, communication, and economic prosperity, while respecting privacy, and guarding against disruption, fraud, and theft."[74]

With this in mind, U.S. policymakers are examining how to adjust existing policies and laws to facilitate the IoT while protecting security and privacy. Given how diffuse the IoT is, this requires input from many agencies and experts. The U.S. Congress formed the Congressional Internet of Things Caucus as a forum for the discussion and education about the policy implications of enabling ubiquitous connectivity and how to simultaneously protect consumers and allow new technologies to flourish.[75]

Caucus leaders have introduced the Developing Innovation and Growing Internet of Things Act (the "DIGIT Act") in the Senate.[76] The DIGIT Act, if enacted, would require the U.S. Department of Commerce to convene a working group made up of federal agencies overseeing various aspects of the emerging IoT sector. The working group will provide recommendations and a report to Congress on the various privacy, security, safety, operational, and economic issues related to the deployment of IoT technologies and potential roles for the federal government to support IoT development while ensuring consumer protections.

Importantly, the Congressional IoT Caucus and the DIGIT Act appropriately recognize that much is unknown about the potential benefits and challenges of the IoT, and the first step in good government is convening experts and developing a robust, factual record. It is imperative for policymakers to fully understand the emerging IoT ecosystem and its many benefits prior to undertaking rulemaking exercises. As Congressional IoT Caucus Co-Chair Congressman Darrell Issa explained, "It's critical that lawmakers remain educated about the fast paced evolution of the Internet of

Things, and have informed policy discussions about the government's role in access and use of these devices."[77]

Top-down, government driven approaches to IoT run the risk of leaving national economies behind those that instead seek to foster policy environments that allow the IoT to develop and flourish. Deployment of 5G networks necessary to support the burgeoning IoT market is underway, and as this advanced mobile footprint expands, so too will the deployment of IoT devices and services. But at this juncture, development of IoT technologies is just beginning. Consumer demand and use cases are still forming. Premature government regulation could undermine this nascent development, threatening to limit IoT's full potential. Policymakers instead need to foster a conducive environment that aids the growth of IoT, while staying informed and gathering evidence that establishes a factual record in support of any policy response that may in the future be merited.

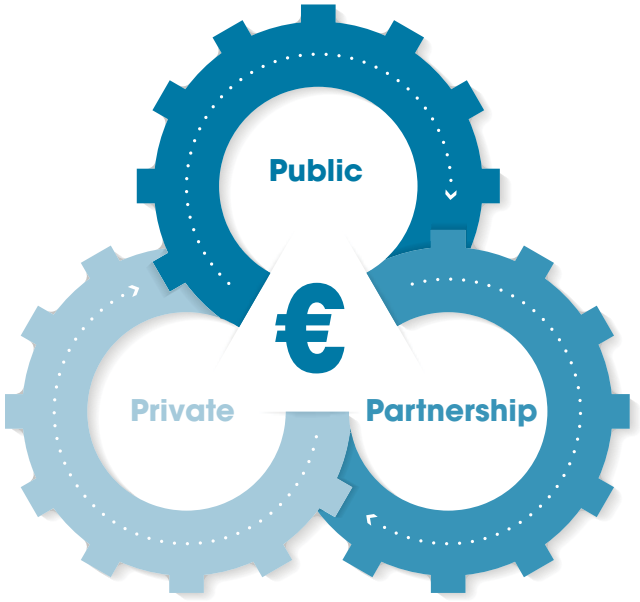
IT IS IMPERATIVE THAT GOVERNMENTS ENCOURAGE A BOTTOM-UP, INDUSTRY-DRIVEN APPROACH TO ENHANCING SECURITY.

The GSMA aptly observes that "the telecommunications industry … has a long history of providing secure products and services to their customers."[78] This success is the result of global, voluntary, and open standards and best practices.

Countries should support these efforts, working collaboratively with industry to identify and facilitate adoption of voluntary best practices. In the United States, for example, the government worked with industry in a year-long collaborative process to develop the *Framework for Improving Critical Infrastructure Cybersecurity* (the framework)—a voluntary, flexible approach that helps organizations understand, manage, and mitigate cybersecurity risks. The framework's concept relies on existing standards, guidelines, and practices to enable organizations to appropriately prioritize investments and conduct risk-based decisions for enhancing security.[79] Gartner reports that in 2015, a mere two years after the framework's release, over 30% of U.S. organizations implemented the framework.[80] Gartner projected 50% of U.S. organizations would implement the framework by 2020.[81]

The EU has similarly engaged with stakeholders to enhance security through its public-private network and information security platform (NIS Platform). Established in June 2013 as part of the EU's Cybersecurity Strategy, the NIS Platform is intended

to "foster the resilience of the networks and information systems which underpin the services provided by market operators and public administrators in Europe" by drawing from international standards and best practices.[82] With participation from industry stakeholders across market sectors, the NIS Platform has working groups to study (i) risk management, including information assurance, risk metrics, and awareness raising; (ii) information exchange and incident coordination, including incident reporting and risk metrics for the purpose of information exchange; and (iii) secure information and communications technology research and innovation.



The EU should continue to encourage multistakeholder engagement and public-private partnerships. These collaborative processes foster the development of voluntary, consensus-based guidance that appropriately takes into consideration the potential effects of such guidance on a wide range of people and interests. During a European Commission-hosted workshop examining the framework and EU NIS Platform approaches, there was wide consensus from the risk management panel "on the need to engage in open, inclusive processes when elaborating frameworks and guidance, thus maximizing the potential for interested organisations to contribute."[83] Public-private partnerships have been the cornerstone of global cyber policy. They are effective because they rely on voluntary consensus standards and industry best practices. The EU and other regions should look for ways to build on existing public-private partnerships and multistakeholder activities.

THERE IS NO ONE-SIZE-FITS-ALL SOLUTION TO IoT CYBERSECURITY.

The IoT is incredibly complex, composed of a range of devices, tags, and sensors, used for a variety of purposes to provide myriad services and to achieve various goals by a complex set of actors—from everyday consumers to large industrial users, from governments to schools, and everything in between. The IoT encompasses services and cloud support as well. No one layer of the ecosystem can solve security.

Cybersecurity threats are similarly complex. A range of bad actors who transcend borders—from nation states to hacktivists—takes advantage of a variety of potential attack vectors and ever-evolving attack technologies to engage in cyberattacks. As CTIA – The Wireless Association describes, "Threat vectors in the growing M2M space are diverse and distributed across broad domains from healthcare and home automation, to energy, transportation and industrial controls. Smartphones and tablets are targets of sophisticated and constantly varying threats. Similarly, threat vectors in the growing M2M space are equally diverse and more complex because of the range of devices that are potential targets for cyberthreats."[84] In short, attack techniques change rapidly and constantly.

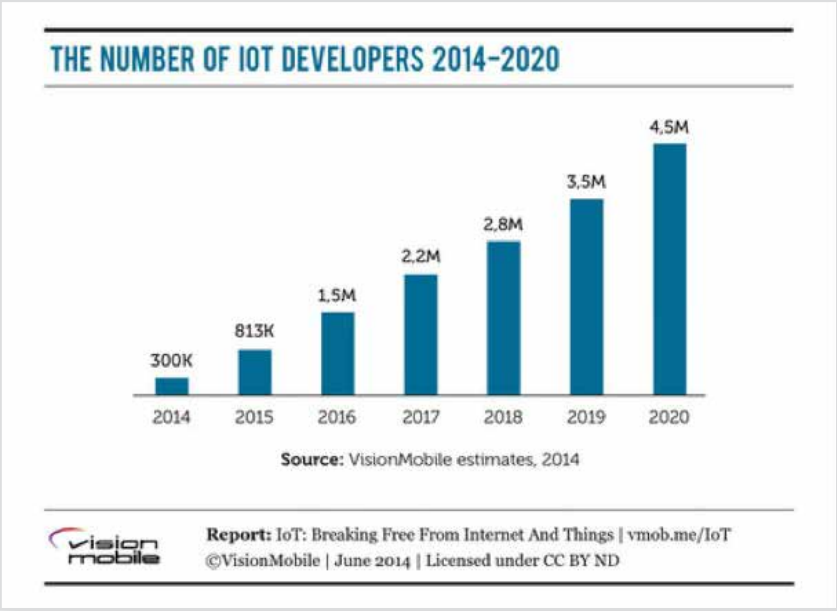
This complexity—regarding the IoT and the ever-evolving threat landscape—defies a "single, prescriptive solution."[85] Instead of a one-size-fits-all solution, which will not work in this ecosystem and threat landscape, governments should look to flexible solutions rooted in risk management, such as building capacity, exchanging threat information, and mitigating risk.

REGULATION OF TECHNICAL STANDARDS WILL BE COUNTERPRODUCTIVE AND BACKWARD-LOOKING.

Governments should avoid picking winners and losers when it comes to technical standards, this is especially true as it relates to cybersecurity, as approaches are continuously evolving alongside threats. What is thought of as a best practice today may become outdated—or worse, ill-advised—tomorrow. For example, long-standing advice about changing passwords has been reconsidered. What once was a best practice is now viewed as counterproductive.[86]

Industry research and development is ongoing, and efforts are running on all cylinders to develop countermeasures to new and evolving threats. Oversight must

remain flexible and technology-neutral in order to both develop solutions to security concerns while also supporting the nascent IoT market. Focusing on a single technical standard—or a set of technical standards—strips resources from entities that are striving to adopt effective, risk-based cybersecurity measures. It also encourages a check-the-box mentality, to cybersecurity, which lulls enterprises into a false sense of security and leaves systems less secure.



Credit: Vision Mobile

Static and cumbersome technical standards that make their way into regulation may hurt businesses' ability to create new jobs. The IoT explosion will lead to job creation at unprecedented levels. VisionMobile projects that job demand for IoT service developers will increase from 300,000 to 4.5 million by 2020—a 57% compound annual growth rate.[87] And there will also be growth in other levels of the IoT market chain, including engineering, manufacturing, and service support. Many of these positions will be security oriented as the need to stay one step ahead of cyber threats will require companies to be vigilant.

Adopting a single set of technical standards can also risk security because no security solutions is able to avoid all vulnerabilities and therefore single approaches, universally adopted, can create a roadmap for bad actors. A "uniform, standardized approach to security challenges … make[s] it easier for cybercriminals to master once and copy endlessly [for] their successful attacks, even turning malware development into cybercrime enterprises on an industrial scale."[88]

GOVERNMENTS SHOULD AVOID CREATING A FALSE SENSE OF SECURITY THROUGH TRUST LABELS, WHICH NEED FURTHER STUDY.

Some governments are exploring labeling to inform the public about security in the IoT. The concept of a trust label needs further study before legislation or regulation is considered. Policymakers need to consider the following principles regarding the potential use of trust labels:

- **Risk-Based:** There are vast differences between IoT use cases, including consumer and industrial IoT uses, and those use cases will require different security measures and privacy protections.

- **Informed by Multistakeholder Consultation:** Multistakeholder and public-private partnerships work because they rely on voluntary consensus standards and industry best practices, and they identify market incentives and investments that foster solutions. These collaborative efforts must include a broad section of industry, consumer, and government stakeholders.

- **Aligned with Existing International Standards:** It is important for existing international standards and standardization to be the cornerstone for security regimes. Governments should support international standards work that can harmonize expectations and technical specifications.

- **Voluntary and Flexible Implementation:** Because IoT uses vary widely and manufacturers desire to sell them globally, it is imperative that governments permit flexible implementation of any trust labels on a voluntary basis. A top-down, one-size-fits-all approach will have limited utility and could have unintended consequences.

Although well intentioned, trust labels may inadvertently discourage end user action. A trust label may lead end users to a false sense of security, which would make end users less likely to take additional security precautions that may be equally critical. The result is a less secure IoT device.

GOVERNMENT CAN BE A CATALYST FOR IoT SECURITY BY FACILITATING COLLABORATION AND EFFECTIVE PARTNERSHIPS.

Consumers, businesses, and government have a shared interest in the global IoT ecosystem and cybersecurity. As ENISA has stated, "the global botnet threat is best countered by close international cooperation between governments and technically-oriented and legislative institutions. For an efficient supranational mitigation strategy to work, cooperation between stakeholders must be intensified and strengthened by political will and support."[89] All countries, across Europe, North and South America, Asia, and Africa should have a shared goal of minimizing botnets, criminal intrusions, fraud, and other nefarious acts. Fortunately, substantial progress has been made to facilitate collaboration in partnerships, and it can be expanded. Some countries, such as Japan, have made collaboration a centerpiece of their cybersecurity policies.[90] National governments should look to a few core activities that they can do now to support collaboration.

Government should support industry collaboration across borders. Within and across countries, public-private partnerships are part of the security picture and should be strengthened and expanded. The Estonian government partnered with 30 public- and private-sector parties as well as academics to develop its recent cybersecurity strategy.[91] The U.S. has championed work by industry sectors to share data via information sharing and analysis centers, information sharing and analysis organizations, and with sector-specific agencies. These models can expand globally if governments devote resources and energy to them.

Government should support international law enforcement collaboration. Recent prosecutions in the United States demonstrate the power of cooperation to increase the costs to those who would compromise the security of our digital economy. Argentina and the United States have formed a cyber policy partnership that would enhance collaboration in cybersecurity, cyber defense, international security in cyberspace, and law enforcement responses to cybercrime, and to strengthen collaboration on cyber issues in relevant international fora.[92] Estonia and the United States formed a similar partnership in 2014, which included bilateral cooperation in law enforcement, academia, internet freedom, and strategic engagement in international fora.[93] The United Kingdom's cybersecurity strategy makes international law enforcement collaboration a priority as well.[94] Such collaborative partnerships will help strengthen law enforcement around the world and mitigate threats.

Government should facilitate and protect vital information sharing. Governments should provide legal certainties to companies that voluntarily choose to share cyber threat information. This will better secure networks and foster more trust between industry and government. Governments should collaborate on information sharing as well as work to align existing domestic regulation from hindering collaboration.

PUBLIC EDUCATION AND EMPOWERMENT ABOUT CYBERSECURITY ARE CRITICAL TO A SECURE DIGITAL FUTURE.

END USER EDUCATION IS KEY TO IoT SECURITY IN OUR BROADER DIGITAL FUTURE.

Consumers may not be prepared for their roles in our digital future, in which individual actions can affect communities and enterprises around the world. This consequence of the Fourth Industrial Revolution presents a major shift and requires thoughtful responses from governments. Nations and regions should consider how to prepare their citizens.

Consumer education is critical. Consumers will play a vital role in securing the IoT ecosystem, including managing their devices, using complex passwords, accepting available upgrades, paying attention to connection security, and installing antivirus software. Use of personal identification numbers, activation of security features, and basic cyber hygiene are critical but often overlooked. Consumers likewise may not prioritize security when purchasing IoT devices or systems.

Enterprise user education will be vital. Consumers are not the only end users who need to adopt better cyber hygiene. Other end users, including enterprises and governments, need to have a better understanding of their roles in the cyber ecosystem and adhere to best practices. Because so many attacks are still perpetrated using low-tech tools like phishing,[95] end users and their devices are critical gateways into larger systems. Large global companies often deploy mobile device management to secure more endpoints. Governments across the world are lagging and should devote energy to smart management of connected devices and raise awareness of existing tools and basic security awareness.

Device manufacturers should be encouraged to support and empower better end user choices. Incentives to produce more secure devices and create more secure networks will line up better if all players have a finer understanding of the ecosystem

and what is at stake. Device manufacturers and vendors should consider how they communicate with consumers and the public about security. Tips for smart device and network use can be provided.

INCREASED NATIONAL AND INTERNATIONAL ATTENTION SHOULD BE PAID TO INDIVIDUALS' ROLES AND RESPONSIBILITIES.

Governments should engage their citizens and build on what works—by embarking on more aggressive national awareness efforts as governments have done with other major social challenges and transitions. As with government action generally, any activity to engage the population should be evidence based, using surveys and behavioral science to focus on what will be effective.

ENISA, the European Commission DG CONNECT, and partners are deploying European Cyber Security Month every October.[96] Likewise, October is cybersecurity awareness month in the United States.[97] Global effort includes "STOP. THINK. CONNECT.™"[98]

According to ENISA, "By deploying a common slogan, logo and awareness messaging suite across all sectors and user cohorts, the STOP. THINK. CONNECT.™ program unifies all enterprises using the campaign's assets into the largest and most resonant awareness program, one that is reinforced repeatedly by design. Since Spring 2014, more than 260 commercial enterprises, educational institutions and NGOs have adopted the campaign."[99]

Research suggests consumer awareness and interest in security is promising, but more globally must be done. Policymakers need to promote educational efforts and take care to avoid unnecessarily alarming consumers or scare them away from using beneficial transformative technology.

If done well, education efforts will not only promote better cyber practices but also generate consumer demand for safer IoT products and services.

CONCLUSION AND KEY PRINCIPLES

Businesses from across multiple sectors are eager to build and leverage IoT solutions to create jobs, expand economies, and improve lives. As one example, in August, the U.S. Chamber of Commerce, along with a coalition of six other organizations—American Chamber of Commerce to the European Union, Confederation of Danish Industry, Confederation of Danish Enterprise, Confederation of Industry of the Czech Republic, EurElectric, and International Chamber of Commerce in Belgium—penned a letter to the European Commission with ideas about how to enhance privacy, security, and trust in the IoT.[100]

> *"We ... look forward to co-creating policies based on existing global, voluntary, consensus, and industry-driven standards; encourage public-private partnerships; and improve security and resilience through public education without creating barriers to growing the IoT ecosystem."*
>
> ***August Coalition Letter***

The business community looks forward to continuing to work with countries around the world to facilitate IoT and other technology innovation. Governments worldwide can promote advancement by prioritizing collaborative partnerships; making data and evidence-based decisions; and avoiding policies that serve as barriers to innovation. As nations and regions consider IoT security and shape our shared future digital economy, policymakers and innovators worldwide should heed several key principles:

TEN KEY PRINCIPLES FOR IoT SECURITY

1. When it comes to security, attempts to regulate today will become outdated tomorrow. Flexible approaches to collaboration and cooperation to combat shared threats have significant advantages over national regulation which serves to fragment the global economy and lags behind technological innovation.

2. Any approach to IoT security should be data-driven, based on empirical evidence of a specific harm, and be adaptable both overtime and cross-border.

3. Security demands should never be used as industrial policy to advance protectionism or favor national economic interests.

4. National boundaries need not become arbitrary obstacles to the movement of devices or data, or to the offering of IoT-related services.

5. Global standards work is the best way to promote common approaches and technology solutions. Such standards should be open, transparent, and technology-neutral.

6. Any government IoT strategy should promote technical compatibility and interoperability to the maximum extent possible.

7. Everybody is vulnerable, cyber threats must be met with global information sharing and collaboration to improve and safeguard the IoT ecosystem.

8. End users need to be educated about their roles and responsibilities in this digital age.

9. Manufacturers and vendors should be encouraged to routinely evaluate and improve endpoint security.

10. The international community must collectively condemn criminal activities that infect and exploit the openness and connectivity of the internet and our digital future. Governments must work together to shut down illegal activities and bring bad actors to justice.

APPENDIX A—SELECT IoT SECURITY STANDARDS ORGANIZATIONS

3GPP is an international partnership that develops standards for cellular telecommunications network technologies. 3GPP's Releases 13 and 14 included technical specifications designed to facilitate secure IoT connectivity.[101]

The Alliance for Telecommunications Industry Standards (ATIS) conducted a study on the different relationships and levels of partnering that may exist between a network operator and an IoT service provider, to illustrate ways to address IoT security concerns.[102]

The Institute of Electrical and Electronics Engineers (IEEE) offers a toolkit with information on myriad IoT issues, including IoT privacy and security,[103] and there is a wealth of technical information from cybersecurity experts in the IEEE Xplore digital library.[104]

oneM2M is a strategic initiative launched by major information and communication technology standards groups throughout the world, including the Association of Radio Industries and Businesses and the Telecommunication Technology Committee of Japan, the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association of the United States, the China Communications Standards Association; ETSI, and the Telecommunications Technology Association of Korea. oneM2M's goal is "to confront the critical need for a common M2M (Machine to Machine) Service Layer, which can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. With an access independent view of end-to-end services, oneM2M will also develop globally agreed-upon M2M end-to-end specifications using common use cases and architecture principles across multiple M2M applications."[105]

Principles for IoT Security

The Online Trust Alliance (OTA) promotes the open development, evolution, and use of the internet for the benefit of all people throughout the world. OTA's mission is to enhance online trust, user empowerment and innovation through convening multi-stakeholder initiatives, developing and promoting best practices, ethical privacy practices, and data stewardship.

The Open Connectivity Foundation (OCF) is dedicated to ensuring secure interoperability for consumers, businesses and industries by delivering a standard communications platform, a bridging specification, an open source implementation and a certification program allowing devices to communicate regardless of form factor, operating system, service provider, transport technology or ecosystem.

The Open Platform Communications (OPC) Foundation. In the manufacturing sector, the OPC Foundation developed the OPC Standard that companies can follow to help enable the secure exchange of data in automated industrial settings. After performing a check of the OPC Unified Architecture's (UA) security functions, the German Federal Office for Information Security confirmed it was designed with security in mind and no systemic security vulnerabilities were found.

Trusted Computing Group (TCG). The Trusted Computing Group (TCG), which is an organization dedicated to creating standards for interoperable trusted computing platforms, is developing the Device Identity Composition Engine (DICE) Architectures for device identification and attestation. This enables manufacturers to use silicon gates to create device identification based in hardware, making security hardware part of the DNA of IoT devices from the ground up.

ABOUT THE AUTHORS:

Megan L. Brown is a partner in Wiley Rein LLP's Telecom, Media & Technology practice. She practices at the intersection of innovation and regulation, helping clients shape policy, respond to investigations, litigate, and develop compliance strategies under federal law, evolving cybersecurity and privacy expectations, state consumer protection law, and varied international regimes. With experience in wireless, satellite, and the Internet of Things, she practices before the Departments of Justice, Homeland Security, and Commerce, as well as the Federal Trade Commission (FTC), Federal Communications Commission (FCC), National Institute of Standards and Technology (NIST), and the National Telecommunications & Information Administration (NTIA). She also helps companies deploy technology by breaking down barriers at the state and local levels.

Wiley Rein Associate **Umair Javed** advises global clients on domestic and international telecommunications and internet regulation, spectrum policy, and privacy and data protection. He works with telecommunications providers, internet and cloud service providers, over-the-top content and application providers, satellite companies, equipment manufacturers, and trade associations. Umair represents clients before the FCC, the FTC, the International Telecommunication Union, the Executive Branch, and foreign regulatory entities.

Wiley Rein Associate **Kathleen Scott** counsels technology clients on regulatory, transactional, and compliance matters. She addresses privacy and cybersecurity issues, and she also advises clients on FCC, FTC, NIST and state law issues. She manages investigations and develops compliance plans. Her areas of focus include FTC privacy and security standards and the Telephone Consumer Protection Act.

Wiley Rein Associate **Madi Lottenbach** counsels technology clients on internet-related issues in the U.S. and abroad, including net neutrality, privacy, cybersecurity, cross-border data flow, and digital trade matters. She advises wireless clients on transactions as well as regulatory and operational requirements and spectrum issues.

Wiley Rein Associate **John Lin** represents technology clients in litigation and regulatory matters. He advises clients on legal, regulatory, and public policy issues that affect the telecommunications and unmanned aerial systems industries, including FCC, Federal Aviation Administration, and state law considerations.

ENDNOTES:

1 Christopher Snow, *All the Ways to Connect Your Kitchen and Laundry Room to Alexa*, Reviewed.com (May 17, 2017), **http://bit.ly/2gV7zGL**.

2 Roberto Baldwin, *The World Now Has a Smart Toaster*, Engadget (Jan. 4, 2017), **http://engt.co/2hSIzhT**.

3 Lauren Goode, *Withings and L'Oreal Have Made a Smart Hair Brush, in the Latest Edition of You're Doing It Wrong*, The Verge (Jan. 3, 2017), **http://bit.ly/2xYmNmd**.

4 Sean Thomas, *Philips Sonicare DiamondClean Smart Brings Bluetooth to Your Brushing*, The Slanted (July 17, 2017), **http://bit.ly/2wT8lNK**.

5 Hewlett Packard Enterprise, *The Internet of Things: Today and Tomorrow* (2016), **http://bit.ly/2cPMuwJ**.

6 Press Release, Gartner, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016* (Feb. 7, 2017), **http://gtnr.it/2l3tOOU**.

7 *Id.*

8 *Id.*

9 i-SCOOP, *IoT – The Complete Online Guide to the Internet of Things*, **http://bit.ly/2eY9SMn** (last visited Aug. 17, 2017).

10 Ericsson, *Ericsson Mobility Report—On the Pulse of the Networked Society*, at 3 (June 2016), **http://bit.ly/25OZI3v**.

11 Press Release, *Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016* (Feb. 7, 2017), **http://gtnr.it/2l3tOOU**.

12 Ericsson, *Ericsson Mobility Report—On the Pulse of the Networked Society*, at 3 (June 2016), **http://bit.ly/25OZI3v**.

13 i-SCOOP, *The Number of Connected Devices by 2021: Impressive Growth Ahead*, **http://bit.ly/2wTgEt3** (last visited Aug. 17, 2017).

14 Telit 2 Market, *The Internet of Things—A New Hope for Europe* (Feb. 26, 2015), **http://bit.ly/2uOfkTJ**.

15 Klaus Schwab, *The Fourth Industrial Revolution*, World Economic Forum (Jan. 14, 2016), **http://bit.ly/1pBfye4**.

16 Bernard Marr, *Why Everyone Must Get Ready for the 4th Industrial Revolution*, Forbes.com (Apr. 5, 2016), **http://bit.ly/2eXUG1w**.

17 Press Release, NTIA, *U.S. Department of Commerce Seeks Comment on Potential Policy Issues Related to Internet of Things* (Apr. 5, 2016), **http://bit.ly/1RV9iZT**.

18 James Manyika et al., *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey Global Institute (June 2015), **http://bit.ly/2xUnfRt**.

19 Deborah Geiger, *Solving the World's Biggest Problems—Possible with IoT, Says Doug Davis of Intel*, SEMI.org (Aug. 4, 2015), **http://bit.ly/2wSWk9s**.

20 *Id.*

21 Intel.com, *Smart Cities UK: Imperial College and Intel IoT Project—The Internet of Things Worldwide with Intel Inside*, **http://intel.ly/2wQLymn** (last visited Aug. 17, 2017).

22 G20 Innovation Report 2016, Prepared for the G20 Science, Technology and Innovation Ministers Meeting, at 44 (Nov. 4, 2016).

23 Report on the 5th Science and Technology Basic Plan, Council for Science, Technology and Innovation, Cabinet Office, Government of Japan, 14 (Dec. 18, 2015) (tentative translation), **http://bit.ly/2m1NtLX**.

24 *Id.*

25 National Cybersecurity Center of Excellence Projects, Use-Cases, *Wireless Infusion Pumps*, NCCoE.NIST.gov, **http://bit.ly/2jgn3cX** (last visited Aug. 17, 2017).

26 Linda, *10 Smart Medical Devices That Are Changing HealthCare 2017*, Appcessories.co.uk (Jan. 10, 2016), **http://bit.ly/2eYfaaK**; *see also* Battelle, *The Big Data Difference: Smart Medical Devices*, HealthcareITNews.com (Jan. 31, 2017), **http://bit.ly/2jqvUIl**; i-SCOOP, IoT – *The Complete Online Guide to the Internet of Things*, **http://bit.ly/2eP8wQo** (last visited Aug. 17, 2017).

27 White Paper, CTIA – The Wireless Association, *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication* (May 1, 2014), **http://bit.ly/2gUH3x4**.

28 Hewlett Packard Enterprise, *The Internet of Things: Today and Tomorrow*, at 11 (2016), **http://bit.ly/2cPMuwJ**.

29 Harnessing the Internet of Things for Global Development, ITU and Cisco, a Contribution to the UN Broadband Commission for Sustainable Development, at 29.

30 *Id.*

31 *Id.*

32 i-SCOOP, *Wearables Market Outlook 2020: Drivers and New Markets*, **http://bit.ly/2xUjz2d** (last visited Aug. 17, 2017).

33 Hewlett Packard Enterprise, *The Internet of Things: Today and Tomorrow*, at 14 (2016),**http://bit.ly/2cPMuwJ**.

34 *Id.* at 8.

35 *Id.* at 8, 10.

36 *Id.* at 9.

37 *Id.*

38 i-SCOOP, *IoT – The Complete Online Guide to the Internet of Things*, **http://bit.ly/2fbIeYW** (last visited Aug. 17, 2017).

39 Anne Morris, *Telefónica Confirms €1.78B UK Smart Meter Deal*, Fierce Wireless (Sept. 25, 2013), **http://bit.ly/2gUduzC**.

40 James Manyika et al., *The Internet of Things: Mapping the Value Beyond the Hype*, McKinsey Global Institute (June 2015), **http://bit.ly/2xUnfRt**.

41 Telit 2 Market, *The Internet of Things—A New Hope for Europe* (Feb. 26, 2015), **http://bit.ly/2uOfkTJ**.

42 Letter from William L. Kovacs, U.S. Chamber of Commerce, to Donald S. Clark, Federal Trade Commission, at 2 (Jan. 10, 2014), **http://uscham.com/2wjchDS** (Regarding the Internet of Things, Project No. P135405).

43 Katie Allen, *Technology Has Created More Jobs Than It Has Destroyed, Says 140 Years of Data*, TheGuardian.com (Aug. 18. 2015), **http://bit.ly/1VHZZ1K**.

44 Zach Supalla, *The Future of the IoT Job Market*, TechCrunch.com (June 10, 2016), **http://tcrn.ch/1WPdZb3**.

45 Ministry of Science, ICT and Future Planning, Ministries of the Republic of Korea, *Master Plan for Building the Internet of Things (IoT) That Leads to the Hyper-Connected, Digital Revolution*, at 3 (May 2014), **http://bit.ly/2xUOYBz**.

46 *Id.* at 5

47 Andrew Meola, *Why IoT, Big Data & Smart Farming Are the Future of Agriculture*, BusinessInsider.com (Dec. 20, 2016), **http://read.bi/2dSXg8a**.

48 *Id.*

49 Libelium.com, Smart Irrigation System to Improve Kiwi Production in Italy (Mar. 13, 2017), **http://bit.ly/2wRp4BS**.

50 White Paper, CTIA – The Wireless Association, *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication*, at 6 (May 1, 2014), **http://bit.ly/2gUH3x4**.

51 NTIA, *Fostering the Advancement of the Internet of Things*, at 17-18 (Jan. 2017), **http://bit.ly/2iMg5Yh**.

52 CTIA, Comment Letter on NTIA's *Fostering the Advancement of the Internet of Things* (Mar. 13, 2017), **http://bit.ly/2gVl64T**.

53 CTIA, *The Next Generation of Wireless: 5G Leadership in the U.S.* (Feb. 9, 2016), **http://bit.ly/2jfnAM1**; Jonathan Fairfield, What Is 5G, When Will It Launch and What Will It Mean for You?, ThaiVisa.com (Jan. 21, 2015), **http://bit.ly/2eYuYtT**.

54 CTIA, *The Next Generation of Wireless: 5G Leadership in the U.S.* (Feb. 9, 2016), **http://bit.ly/2jfnAM1**.

55 *Id.*

56 Communications Sector Coordinating Council, *Industry Technical White Paper* (July 17, 2017), **http://bit.ly/2xozz09**.

57 *Id.*

58 Press Release, *Gartner, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016* (Feb. 7, 2017), **http://gtnr.it/2l3tOOU**.

59 Symantec, *An Internet of Things Reference Architecture* (Feb. 2016), **http://symc.ly/2wQSmAl**.

60 ENISA, *Botnets: Ten Tough Questions* (Mar. 7, 2011), **http://bit.ly/2eOaH6s**.

61 ENISA, *EU Operational Cooperation Under Test for the Second Time* (July 3, 2017), **http://bit.ly/2udmfcU**.

62 ETSI, *Internet of Things—Our Role & Activities*, **http://bit.ly/2eWQBuE** (last visited Aug. 17, 2017).

63 GSM Association, *GSMA IoT Security Guidelines—Complete Document Set* (Feb. 9, 2016), **http://bit.ly/2wTuZUk**.

64 GSM Association, *GSMA IoT Security Guidelines—Overview Document, Version 1.1* (Nov. 7, 2016), **http://bit.ly/2gVZMMF**.

65 GSM Association, *GSMA IoT Security Guidelines—Service Ecosystems, Version 1.1* (Nov. 7 2016), **http://bit.ly/2wiPB6J**.

66 GSM Association, *GSMA IoT Security Guidelines—Endpoint Ecosystems, Version 1.1* (Nov. 7 2016), **http://bit.ly/2eX0fgP**.

67 GSM Association, *GSMA IoT Security Guidelines—Network Operators, Version 1.1* (Sept. 2016), **http://bit.ly/2xoMpLM**.

68 GSM Association, *IoT Security Assessment Process* (2016), **http://bit.ly/2jf77Yq**.

69 GSM Association, *Solutions to Enhance IoT Authentication Using SIM Cards* (UICC) (Nov. 2017), **http://bit.ly/2vObNpK**.

70 GSM Association, *Securing the Port of the Future: Secure IoT Solutions for the Smart City* (Apr. 2017), **http://bit.ly/2wTkWAq**.

71 *Id.* at 2.

72 IEEE, IEEE Internet Policy Community White Paper: Internet of Things (IoT) Security Best Practices (Feb. 2017), **http://bit.ly/2xYvHQF**.

73 Exec. Order No. 13563, *Improving Regulation and Regulatory Review*, 76 Fed. Reg. 3821 (Jan. 18, 2011), **http://bit.ly/2eOU36M**.

74 Exec. Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22391 (May 11, 2017), **http://bit.ly/2wT5jHI**.

75 Press Release, *U.S. Reps. DelBene and Issa Announce Creation of the Congressional Internet of Things Caucus* (Jan. 13, 2015), **http://bit.ly/2gWcfzG**.

76 Developing Innovation and Growing the Internet of Things Act, S. 81, 115th Cong. (2017), **http://bit.ly/2jfpVH2**.

77 Press Release, *U.S. Reps. DelBene and Issa Announce Creation of the Congressional Internet of Things Caucus* (Jan. 13, 2015), **http://bit.ly/2gWcfzG**.

78 GSM Association, *GSMA IoT Security Guidelines—Overview Document, Version 1.1* (Nov. 7, 2016), **http://bit.ly/2gVZMMF**.

79 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0* (Feb. 12, 2014), **http://bit.ly/2jSGfcQ**. The National Institute of Standards and Technology (NIST) has released a draft update to the Cybersecurity Framework and is in the process of reviewing public comment on proposed edits and additions. *See* NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1* (Jan. 10, 2017), **http://bit.ly/2wQXHrz**.

80 *See* NIST, *Cybersecurity "Rosetta Stone" Celebrates Two Years of Success* (Feb. 18, 2016), **http://bit.ly/2vOEPpo**.

81 *Id.*

82 ENISA, *NIS Platform*, **http://bit.ly/2fc48eG** (last visited Aug. 17, 2017).

83 ENISA, *Summary Report: Preliminary Workshop Comparing U.S. Cybersecurity Framework and EU NIS Platform Approaches*, at 1 (Nov. 2014), **http://bit.ly/2eXX7Bi**.

84 White Paper, CTIA – The Wireless Association, *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication*, at 12 (May 1, 2014), **http://bit.ly/2gUH3x4**.

85 NTIA, *Fostering the Advancement of the Internet of Things*, at 26 (Jan. 2017), **http://bit.ly/2iMg5Yh**.

86 Lorrie Cranor, *Time to Rethink Mandatory Password Changes*, Tech@FTC Blog (Mar. 2, 2016) **http://bit.ly/1To5jaj**.

87 Matt Asay, *The Internet of Things Will Need Millions of Developers by 2020*, ReadWrite.com (June 27, 2014), **http://bit.ly/2xf6YcP**.

88 White Paper, CTIA – The Wireless Association, *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication*, at 12 (May 1, 2014), **http://bit.ly/2gUH3x4**.

89 ENISA, *Botnets: Detection, Measurement, Disinfection and Defence* (Mar. 7, 2011), **http://bit.ly/2wiXZmw**.

90 Government of Japan, *Cabinet Decision: Cybersecurity Strategy* (Sept. 4, 2015), **http://bit.ly/2xogQlv**.

91 Anna-Maria Osula, NATO Cooperative Cyber Defence Centre of Excellence, *National Cyber Security Organisation: Estonia* (2015), **http://bit.ly/2xpu15E**.

92 U.S. Department of State, Joint Statement on *U.S.-Argentina Partnership on Cyber Policy* (Apr. 27, 2017), **http://bit.ly/2wTe4RS**.

93 U.S.-Estonia Cyber Partnership Statement (Dec. 3, 2013), **http://bit.ly/2xUg6Re**.

94 HM Government, *National Cyber Security Strategy 2016–2021* (Nov. 1, 2016), **http://bit.ly/2gdBbhS**.

95 Stop. Think. Connect., *How Phishing Works* (June 15, 2017), **http://bit.ly/2vYxVCa**.

96 European Cyber Security Month, *What Is ECSM?*, **http://bit.ly/1PLrmCi** (last visited Aug. 17, 2017).

97 U.S. Department of Homeland Security, *National Cyber Security Awareness Month* (Aug. 11, 2017), **http://bit.ly/2bmwhxv**.

98 Stop. Think. Connect., **http://bit.ly/1R26Gql** (last visited Aug. 17, 2017).

99 European Cyber Security Month, *More ICT Campaigns*, **http://bit.ly/2fbEvL1** (last visited Aug. 17, 2017).

100 U.S. Chamber of Commerce, *IoT Cybersecurity Coalition Letter* (Aug. 16, 2017), **http://uscham.com/2vRsgw2**.

101 Philippe Reininger, 3GPP *Standards for the Internet of Things* (Nov. 2016), **http://bit.ly/2xfbMyC**; 3GPP, 3GPP Work Items Associated with Specification (Aug. 1, 2017), **http://bit.ly/2gVdqvO**.

102 ATIS, *Securing Internet of Things (IoT) Services Involving Network Operators* (May 2017), **http://bit.ly/2eP4zuX**.

103 IEEE, *Internet of Things Toolkit* (2017), **http://bit.ly/2wTgqjF**.

104 IEEE, *Xplore Digital Library*, **http://bit.ly/1reWJYP** (last visited Aug. 17, 2017).

105 ATIS, *About oneM2M*, **http://bit.ly/2xV0ywo** (last visited Aug. 17, 2017).

U.S. CHAMBER OF COMMERCE

1615 H Street NW | Washington, DC 20062