AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

DANSK ERHVERV
CONFEDERATION OF DANISH ENTERPRISE

DI
Confederation of Danish Industry

SP
CONFEDERATION OF INDUSTRY OF THE CZECH REPUBLIC

eurelectric
ELECTRICITY FOR EUROPE

ICC BELGIUM
INTERNATIONAL CHAMBER OF COMMERCE
The world business organization

U.S. CHAMBER OF COMMERCE

August 17, 2017

Mr. Andrus Ansip
Vice President for Digital Single Market
European Commission
Rue de la Loi, 200
B-1049 Bruxelles
Belgium

Ms. Mariya Gabriel
Commissioner for Digital Economy and Society
European Commission
Rue de la Loi, 200
B-1049 Bruxelles
Belgium

Dear Vice President Ansip and Commissioner Gabriel:

In advance of the European Union (EU) review of its Cybersecurity Strategy, which will include "measures on cyber security standards, certification and labelling, to make ICT-based systems, including connected objects, more cyber secure,"[1] our organisations are writing to contribute our thoughts on how to enhance privacy, security, and trust in the Internet of Things (IoT).

Our organisations represent companies of all sizes and from all sectors of the economy. We write to you having incorporated the views of manufacturers, service providers, the electricity industry, and standard-setting bodies that are at the forefront of cybersecurity innovation and will lead the global effort to make connected devices cyber secure. The transatlantic marketplace is a natural place for EU and U.S. firms to do business. Our members support hundreds of thousands of jobs underpinned by digital trade in each other's markets. The EU and U.S. have a shared interest in leading a global digital economy based on openness, innovation, and access while safeguarding consumers, security, and privacy.

Our members remain committed to complying with existing and future EU rules around privacy, security, and trust and to do so effectively and efficiently.

IoT—An Imminent Revolution

The presence of IoT objects is rapidly expanding, connecting humans and machines with technology to improve their lives and increase the efficiency of industrial operations. It is estimated that there will be more than 50 billion connected devices by 2020, over 30 times the number in 2009.[2] Within the EU alone, the number is estimated to increase from approximately 1.8 million in 2013 to almost 6 billion in 2020.[3]

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee on the Regions on the *Mid-Term Review on the implementation of the Digital Single Market Strategy*, May 10, 2017. http://bit.ly/2pvCoUG

[2] Dave Evans, Cisco, April 2011, *The Internet of Things: How the Next Evolution of the Internet is Changing Everything*. http://bit.ly/1LgfMSb

[3] IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, study for the European Commission. http://bit.ly/2uOfkTJ

This brings with it “the potential to unleash significant economic growth across … the world.”[4] By some accounts, “the IoT has a total potential economic impact of $3.9 trillion to $11 trillion a year by 2025.”[5] In the EU alone, the market for IoT objects is projected to reach more than €1 trillion by 2020.[6]

The greatest benefits of the IoT will be realized by the users of connected devices. Consumers will benefit from being able to manage their health, run their homes, and improve their quality of life in new and innovative ways. Businesses will benefit from more efficient systems and supply chains—providing better service to their customers while reducing unnecessary waste and improving sustainability goals. This has to happen in full compliance with the General Data Protection Regulation (GDPR) and respect for customers’ privacy. The IoT also brings with it the potential for large-scale job creation. Vision Mobile projects that 4.5 million developers worldwide will contribute to the IoT by 2020.[7]

Given Europe’s position as a global leader in technology, it can expect to benefit from increased job creation and economic growth brought by the IoT, as long as it maintains a policy environment that supports innovation and growth.

Smart Regulation for Smart Devices

Leading industry stakeholders recognize the importance of privacy and security. We urge all stakeholders to make privacy, security, and trust in the IoT ecosystem a priority, not simply for security’s sake but for the end-to-end well-being of the entire ecosystem.

It is critical that as regulators act to promote a cyber secure ecosystem and they do not advance policies that inadvertently stifle innovation. The vast potential of the IoT will be realized only in a policy climate that focuses on managing risk, not blocking change. We urge policymakers to avoid regulations that may lead to gold plating or fragmentation across the European market.

There is no silver bullet to managing the security of the IoT ecosystem. The myriad, fast-moving threats that seek to compromise the IoT are borderless and include nation-states, organized crime, hacktivists, and terrorists that businesses cannot tackle alone. Therefore, we propose to focus on the following six principles that raise cyber defenses and realise the potential of the IoT.

1. Resist the Urge to Regulate the IoT Prematurely

We are convinced that cyber risk in the IoT ecosystem is an extension of current risks in network and information systems. As such, risks to confidentiality, integrity, and availability of data apply, meaning that IoT-specific mandates or guidance, including ones related to privacy and security, are not needed at this time as they are covered by existing and forthcoming EU legislation.

[4] Amanda Eversole, U.S. Chamber of Commerce, March 2, 2016, *We’ve Been Talking About the Internet of Things All Wrong*. http://uscham.com/2uxOgZy

[5] McKinsey Global Institute, June 2015, Report: *Unlocking the Potential of the Internet of Things*. http://bit.ly/2wBZ9LE

[6] IDC and TXT Solutions (2014).

[7] Available at: http://bit.ly/2fyRiKH

The General Data Protection Regulation (GDPR) will require all businesses and, more specifically, IoT providers to implement new methods and technologies for the protection of personally identifiable information and security. Under the GDPR, "data protection by design and by default is an essential principle."[8] In parallel, the Network and Information Security (NIS) Directive raises baseline security measures for operators of essential services and digital service providers, including IoT providers that leverage cloud computing services. These are also complemented by the existing Telecoms regulatory framework's security obligations and the ePrivacy Directive data breach obligations both currently under review.

A considered and thoughtful approach is needed here and we commend the Alliance for the Internet of Things Innovation's (AIOTI) Working Group 4 (policy) conclusion that "any regulatory proposal targeting the IoT should address only well-defined market failures that cannot be addressed through existing law and self-regulatory measures."[9]

2. Leverage Existing Best Practices and Global Industry-Led Standards

Efforts to improve the privacy and security of IoT objects should reflect the borderless and interconnected nature of the digital environment. Standards, guidance, and best practices relevant to cybersecurity are most effective when developed and recognized globally. This avoids burdening multinational enterprises with the requirements of conflicting jurisdictions while facilitating interoperability, compatibility, reliability, and security on a global scale.
For these reasons, the NIS Directive explicitly directs member states to "encourage the use of European or internationally accepted standards and specifications relevant to the security of network and information systems."[10]

Pioneering businesses are working together on developing privacy and security solutions; collecting open, consensus-driven standards; and innovating business models. We urge businesses to share and publicize case studies of how they have used global, voluntary, consensus-based, and industry-led standards within their IoT object development. These efforts would be stymied by the slow and unitary nature of the EU standards development process should the EU move forward with mandatory standards, testing, and labelling requirements. Meanwhile, threat actors will continue to innovate unhindered.

International policymakers should align IoT security programs with industry-backed approaches to risk management, such as the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (the framework). The framework is biased toward a standards- and technology-neutral approach to managing cyber risks.

[8] European Commission, April 6, 2016, *General Data Protection Regulation*. http://bit.ly/1YsdUHB

[9] Alliance for the Internet of Things Innovation (AIOTI), *Report AIOITI Working Group 4 – Policy*, October 15, 2015. http://bit.ly/2vWsfbn

[10] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). http://bit.ly/2a6gFgw

3. Avoid a One-Size-Fits-All Approach

Employing one-size-fits-all standards, certifications, and labelling requirements for connected devices does not seem the right match to confront face-paced commercial demands and risks that companies face online. Such an approach would place unnecessary burdens on industry, especially small and midsize enterprises, driving up the cost of devices while offering no greater security.

Rather, we invite the Commission to collaborate with industry to manage the risks inherent to each device, understanding that the risks to complex or niche industrial devices are different than consumer devices. In particular, as more traditional products and services depend on data to function, it is important that a holistic view is adopted. Wearables, drones, and autonomous vehicles are just the beginning of the possibilities that these relationships could forge.

A flexible, collaborative approach to privacy and security, including capacity building, exchanging threat information, and managing risk, has proven to be more effective than mandating information-security requirements. Different sets of flexible cybersecurity best practices will be relevant for different IoT audiences, ranging from producers to network operators to users. Cumulatively, this approach will ensure that hazards to businesses' cybersecurity do not pool at any given point.

4. Avoid Creating a False Sense of Security Through Trust Labels

The European Commission[11], the European Cyber Security Organisation (ECSO), and the European Union Agency for Network and Information Security (ENISA) are discussing the possibility of mandating the use of an IoT trust label. The primary goal of a trust label is twofold: to improve product security and better inform consumers. Cybersecurity is a dynamic and evolving threat, and we believe that further study is needed before a decision is taken whether to move forward.

The IoT is still an emerging technological area in the earliest days of its development and growth. The EU must enable an environment that allows safe, responsible innovation, and does not unintentionally limit innovation, hinder market access, or undermine European competitiveness compared to the rest of the world.

Full use should be made of existing instruments (e.g., GDPR, eIDAS Regulation, and the NIS Directive) to address any concrete and proven issues or market failures that may arise in the IoT space. These nascent technologies, whose future attributes, properties, performance, and possible uses cannot even be anticipated yet, should not be subject to rigid, prescriptive, and unnecessary regulation. Specifically, we remain concerned that pushing for generic or blanket cybersecurity labelling of IoT products could result in counterproductive technology mandates, new market access barriers, or roadblocks to innovation without necessarily bringing any real security or privacy benefits that could not otherwise be achieved on the basis of already existing instruments.

[11] European Commission, April 19, 2016. Staff Working document *Advancing the Internet of Things in Europe.* http://bit.ly/2wQ54vR

5. Be a Catalyst for Innovation in IoT Security by Convening Public-Private Dialogues

Industry and government on both sides of the Atlantic must work collaboratively to drive the use of privacy- and security-by-design practices. The Commission is well placed to facilitate these conversations at the EU level and ensure participation from leading cyber actors.

The Commission has already launched a number of such initiatives within the EU. We would welcome efforts to expand these discussions to incorporate the views of international government and industry stakeholders, whose expertise would no doubt add value to these discussions. We applaud the Commission's call to "enhance its international cybersecurity cooperation with EU's main trade partners to work towards stronger cybersecurity for connected objects"[12] and stand ready to assist in its effort.

In addition, more should be done to facilitate cyber information sharing—a proven method for increasing information security. We respectfully urge the Commission to provide legal certainty to companies sharing cyber threat information in real time with industry peers or government entities so that they are protected from liability, disclosure, and regulatory action. This will facilitate greater participation in information-sharing forums, enhance trust between government and industry in the battle against cyber adversaries, and advance cybersecurity in the IoT ecosystem.

6. Improve Public Education About Cybersecurity

In addition to advancing IoT cybersecurity, it is necessary to increase awareness among consumers about cybersecurity. As with information security networks more generally, the greatest vulnerability to the IoT ecosystem is human error—whether clicking on phishing links, failure to update or patch systems, or lack of adherence to basic practices of cyber hygiene.[13]

Within industry, not every business—especially small and midsize businesses—has the knowledge and expertise to make smart decisions about security when developing and deploying IoT devices and services. Technical innovations like encryption, pseudonymisation, and anonymisation hold privacy and security value to protecting data and may be voluntarily adopted by IoT providers.

As such, even modest improvements in public awareness of, and attitudes towards cybersecurity can drastically improve IoT security. Investments in education and awareness campaigns by the Commission can help increase the scale and impact of existing industry-led efforts.

Owners of connected devices need to be aware of the importance of installing software updates, using strong passwords and, in relevant cases, installing other security-enhancing tools —not only for their own benefit but for the benefit of the IoT ecosystem as a whole. Small and midsize enterprises, meanwhile, should be adequately supported in implementing best practices introduced by their more sophisticated peers in government and industry.

[12] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee on the Regions on the *Mid-Term Review on the implementation of the Digital Single Market Strategy*, May 10, 2017. http://bit.ly/2pvCoUG

[13] BakerHostetler, *Is Your Organization Compromise Ready? 2016 Data Security Incident Response Report*. http://bit.ly/2hRsPkh

To be sure, the expansion of the digital economy is a good thing with the potential to increase significant gains across the continent. Governments, users, and businesses must work together to manage cyber risks to unleash the full potential of the IoT.

Conclusion

Company owners and operators view privacy and security as crucial and as an essential part of risk management. They guard their business operations from interruption; prevent the loss of personally identifiable information, capital, and intellectual property; and protect public safety. Businesses routinely strive to strengthen the security of their information systems and identify and mitigate any network or system vulnerability, which requires greater public-private cooperation and information sharing.

Our organisations welcome the EU's focus on enhancing privacy, security, and trust for IoT objects. The EU has made progress on improving security and resilience since the first EU Cybersecurity Strategy was issued in 2013. Recent policies like the GDPR and the NIS Directive build on this foundation. But cyberattacks will increase in scale, sophistication, and frequency and will pose a threat to privacy and security of public and private institutions and consumers on both sides of the Atlantic. Future policy proposals should embrace collaboration, flexibility, and innovation over the long term—enabling solutions to advance at the pace of the market.

Governments and the private sector need to join forces to deflect and defeat increasingly sophisticated and persistent adversaries. Further, our organisations welcome the opportunity to work with the EU to craft policies to enhance current information-sharing practices between government and the business community and reflect the conditions of an increasingly digital world.

Every organisation, industry, and government faces cyber threats, and none of us are immune to their disruptive potential. Businesses genuinely want government partners in the fight against organized criminal gangs, hacktivists, and groups carrying out state-sponsored attacks. We need a mind-set that we are all in this together.

We appreciate your consideration of our concerns and 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.

Signed,

American Chamber of Commerce to the European Union
Confederation of Danish Industry
Confederation of Danish Enterprise
Confederation of Industry of the Czech Republic
EurElectric
International Chamber of Commerce in Belgium
United States Chamber of Commerce