Building trust in IoT security through legislation

Version 2.0

CRYPTO QUANTIQUE

Contents

Introduction

Securing the Internet of Things (IoT) is a challenge. Think of what is involved in deploying an IoT ecosystem: building or buying a lot of low-cost autonomous sensing devices, distributing them to arbitrary locations, and then having them communicate over arbitrary channels. With billions of IoT devices already in the field and many more being deployed, the potential for security breaches is enormous.

Reducing the chances of a breach involves a combination of hardware, software, standards, certifications, business processes and legislation, which together can help build trust in IoT ecosystems. The challenge is that the IoT is such a broadly drawn concept that there is a lot of overlap between current and new approaches to addressing IoT security; among these approaches to building trust; and between potential arbiters of trustworthiness such as standards bodies, governments, and industry groups. These organizations will have to develop a lot of trust amongst themselves if they truly want to weave today's patchwork of actions into the whole cloth of a secure IoT.

The legal context

IoT devices and ecosystems are already subject to significant legislation since they have been introduced into a world in which issues such as data privacy and product liability are already well regulated. This means that IoT companies face serious financial and reputational risks if their work is found to be non-compliant. Penalties may include fines, personal liability and even imprisonment for those responsible for security breaches, as well as the possibility of facing cease-and-desist orders, erasure of data, product recalls, and the imposition of additional security measures. Other costs involved with non-compliance can include damages, repair schemes, audits, and the possibility of losing the right to act in a market.

To add some meat to the bones, the European Union's General Data Protection Regulation (GDPR) specifies a maximum fine for breaches of up to €20 million, or 4% of global turnover, whichever is greater. Those who violate America's Federal Trade Commission Act could face fines of $41,484 *per violation, per day* – which means that if an organization has a systemic security breach in a large IoT ecosystem, fines can mount up quickly. And consider the logistic challenge of resolving a data breach: in Australia, the Privacy Act 1988 and the Notifiable Data Breaches Act 2017 require that organizations whose products or services suffer a data breach must automatically tell all the affected users about it.

In 2018, the IoT Security Foundation provided a useful insight into the details of some of the key regulatory frameworks in place for the IoT worldwide, as follows:

European Union

The three key regulations applying to the sale and use of IoT devices and ecosystems at that point were CE Marking, the GDPR, and the Network and Information Security Directive (NIS Directive).

CE Marking addresses the safety, health and environmental impact of products sold in the EU, and is governed by evolving product categories and regulations. CE Marking can affect both IoT devices and the organizations providing them, whether they are makers, importers or distributors, all of which are liable for ensuring compliance with CE Marking. Some of the sanctions for not meeting CE Marking requirements can include having the product removed from the market, penalties, fines, and imprisonment.

GDPR is well established now. The body responsible for complying with GDPR in an IoT ecosystem is likely to be a direct provider such as a device maker; a utility provider such as an ISP; or a digital service provider such as a cloud service. GDPR regulations apply to product developers and manufacturers, even if they are not acting as an IoT provider. And a GDPR compliance risk can emerge in IoT ecosystems if, in dealing with personal information, the roles of data controller and data processor are handled by one organization, rather than being split so that there is some useful tension between the two roles.

The NIS Directive only applies to IoT providers designated as either an Operator of Essential Services such as gas, electricity and water, or a Designated Service Provider such as an online marketplace, search engine or cloud service.

United States

The three key acts relevant to the IoT in the US are the Federal Trade Commission Act (FTC Act), the Cyber Security Information Sharing Act (CISA), and the Children's Online Privacy Protection Act (COPPA).

The FTC Act regulates anti-competitive behavior such as unfair or deceptive practices. The FTC has already brought cases against IoT device makers that failed to ensure the security of their products. And it looks likely that the FTC Act will still apply to US IoT providers if their products or services are deployed outside the US. Sanctions can include restitution to victims, audits, product recalls, and federal or state civil lawsuits.

CISA is meant to encourage the sharing of cybersecurity information, and so voluntarily participating in CISA activities can relieve organizations of some legal liabilities, as well as providing some protection from the Freedom of Information Act.

COPPA is used to protect children's data and to shield them from targeted content online. Under COPPA, IoT providers should not knowingly collect children's data, should anonymize or pseudonymize any data they do collect, and ensure that any third parties that they hire do the same. The challenge for the IoT provider in this context is to ensure that any cloud or web services with which they work are not collecting children's data by accident or default.

United Kingdom

Three key acts apply in the UK: the Data Protection Act 2018 (DPA), the Consumer Rights Act 2015 (CRA), and the Digital Economy Act (DEA).

The DPA implements the GDPR in the UK. It also includes provisions that protect subjects' rights from decisions with legal or significant impact, if those decisions have been made by automated systems. This may be particularly relevant to IoT providers as their services are often sold on the basis of their ability to automate processes. Companies that are in breach of the DPA can be searched, fined, and have their data forfeited or erased. Directors or managers can also be held personally liable.

An update to the CRA in 2015 added a section that defined digital content as 'data produced and supplied in digital form', which must be of 'satisfactory quality'. The implication here for IoT providers is that they need to ensure that their products and services will continue to work properly for years after they are sold and that they could be held liable for the impact of low-quality digital content – such as devices that are shipped or infected with malware.

The DEA has provisions that are relevant to suppliers of specific types of IoT goods and services, such as for use in digital infrastructure, which may affect IoT providers that manage networks, or access to the internet and online content. IoT providers in the utility sectors are also subject to information-sharing and processing requirements under the DEA.

Australia

There are three key acts relevant to the IoT in Australia: the Privacy Act 1988; the Notifiable Data Breach Act (NDB Act); and the Competition and Consumer Act 2010 (CCA).

The Privacy Act sets out 13 principles for companies handling personal information. Of these, IoT providers need to be particularly aware of the principles relating to anonymity, pseudonymity, and the security, use or disclosure of personal information, especially across borders. If your IoT ecosystem does send personal information out of Australia, you are responsible for ensuring that the overseas organization which receives it sticks to Australian privacy principles.

The NDB Act piles on the pressure by requiring companies to tell the Office of the Information Commissioner within 30 days if they suffer a data breach that could cause an individual serious harm. As previously discussed, the company must also tell the affected individuals or provide a public statement if it suffers a notifiable data breach. It's a product lifecycle management issue that is probably not well addressed by some IoT players: it seems unlikely that the makers of a cheap fitness tracker would be willing or able to reach out to their customers a few years after they had made the device.

The CCA is somewhat like the UK's CRA, in that it demands that products must be fit for purpose, free from defects and safe. IoT developers can demonstrate they are trying to meet the standards by using encryption to protect personal information, and ensuring they can patch and update firmware and software to keep the product free from defects. The Act also calls for products to be repairable for a reasonable amount of time after purchase.

Singapore

Singapore inherits some of its IoT-relevant legislation from the UK under the Application of English Law Act (AELA). Other relevant acts include the Energy Conservation Act (ECA) and the Health Products Act (HPA).

The AELA was first enacted in 1993 to clarify the extent to which English law is applicable in Singapore, and has been through two updates. IoT providers should note differences in commercial law between the UK and Singapore, particularly covering insurance, the supply of goods and services, and unfair contract terms.

The ECA defines energy management and conservation practices in Singapore. It applies to any IoT product that requires electricity or fuel, and which interacts with at least one other device. The challenge for IoT providers is that if an overall system does not meet the required energy efficiency standard, then they must find a way of ensuring it does. This could mean extra costs for IoT providers who add their technology to an existing system.

The HPA regulates the manufacture, import, supply, storage, presentation and advertisement of health products. It covers IoT products such as medical robots, implantable glucose monitors and pacemakers, portable medical devices, and cosmetic devices such as toothbrushes and laser hair removers. If such a product has a defect or creates an adverse effect, it must be reported. Because the definition of defect is so broad, products could be taken off the market if they had a vulnerability that turned out to be impossible to patch.

The emergence of IoT-specific legislation

New legislation has been developed since 2018 that will more directly apply to the IoT.

European Union

On 21 March 2019, the European Union adopted the Cybersecurity Act. This gives ENISA, the European Union Agency for Cybersecurity, a permanent mandate. The Act also establishes an EU framework for cybersecurity certification, to ensure a common approach across the internal market. The idea is to improve cybersecurity in a broad range of digital products, including IoT devices and services.

California

On 1 January 2020, California enacted a law designed to protect the privacy of personal information being shared through connected devices. The bill requires that IoT device makers give their devices security features to protect any information they collect or share from unauthorized access, destruction, use, modification, or disclosure. The bill goes on to say that every such device should have a unique, pre-programmed password, or a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

South Korea

South Korea has focused its cyber-legislation around protecting personal information. Its Personal Information Protection Act (PIPA) says that companies must take physical, technical and administrative measures to prevent personal information from being lost, stolen, leaked, or tampered with. They must have a formal statement of these measures. They must appoint a privacy officer to oversee any personal data processing, and that person is responsible for any infringement. In the event of a data breach, a company must notify the authorities and all the data subjects.

In February 2020, the Korea Internet and Security Agency published guidelines that applied the requirements of PIPA to the development of IoT ecosystems, particularly those that handle personal information. It based these on the concept of Privacy by Design, which involves thinking about how personal information is used right from the service planning and design stage. For example, during planning, designers should work out whether they need personal information, and if so, check that the way they are collecting and using that information is legal.

The introduction of these guidelines is seen by some as a shift from South Korea's previous, more laissez-faire approach to the IoT, which was meant to accelerate its uptake in the country.

United Kingdom

The UK has been consulting on how to introduce cybersecurity laws to protect smart devices and IoT infrastructure for the past couple of years. In April 2021 it announced its plans to legislate, based on feedback from the consultation. Under the planned legislation, customers must be informed, at the point of sale, for how long a smart device will receive security software updates. Manufacturers will also be banned from shipping products with default passwords and will have to provide a public point of contact to make it simpler for anyone to report a vulnerability. An enforcement body will be established and given the power necessary to investigate allegations of non-compliance and ensure compliance.

This work is part of a wider, longer-term push by the UK government to improve cyber security, which goes back to the launch of a National Cyber Security Strategy in 2016. Among the stated goals of that Strategy were to ensure that the majority of online products and services were 'secure by default' by 2021.

The Strategy was followed up in 2018 with the publication of a Code of Practice for Consumer IoT Security, which set out the security principles that should be applied by manufacturers and others involved in the market. The Code includes 13 major guidelines, and applies to consumer IoT products that are connected to the internet, and/or to a home network, and associated services. It defines 'associated services' as digital services linked to IoT devices, such as mobile apps, cloud computing and storage, and third-party application programming interfaces to services such as messaging.

While this Code of Conduct was in development, the UK was also contributing to the development of a European standard, EN 303 645. Handily, there's a direct mapping between many of the guidelines in the Code of Conduct and clauses in the EN 303 645 standard, so if a manufacturer complies with one they also comply with the other. Similar standards are being developed in other parts of the world, with increasingly common requirements, which should ease the burden of compliance for companies making products for global markets.

The proposed legislation will apply to consumer-connected products and smartphones. The government policy paper on the legislation lists some the products that fall within the scope of its intended regulation, as follows:

- Smartphones
- Connected cameras, TVs and speakers
- Connected children's toys and baby monitors
- Connected safety-relevant products such as smoke detectors and door locks
- Internet of Things base stations and hubs to which multiple devices connect
- Wearable connected fitness trackers
- Outdoor leisure products, such as handheld connected GPS devices that are not wearables
- Connected home automation and alarm systems
- Connected appliances, such as washing machines and fridges
- Smart home assistants

The policy document also lists some products which will not be subject to the legislation. These include smart meters, which it sees as already being heavily regulated, and laptops, desktops and unconnected tablets, because of the complexity of making such flexible devices comply with the security requirements. The legislation will also not cover second-hand products, because it is deemed impractical to do so.

The policy document says that when it asked for comments on its proposals in July 2020, the government planned to exempt cars, electric car chargers, and medical devices from the legislation to avoid a clash with other regulations. Because the regulatory landscape for these products has changed since then, the government may want its legislation to cover them in future. The intended legislation will therefore give Ministers the right, with the agreement of Parliament, to adjust the type of consumer connected products that it covers. Manufacturers of currently exempt products may want to address security issues in their products now, to defend against having to comply with updated UK legislation at short notice.

As previously discussed, the proposed legislation is focused on three quick security fixes: banning the use of default passwords; enabling vulnerability reporting; and telling customers how long a manufacturer plans to maintain the security of a device. Ministers plan to reserve the right to update the security requirements and designated standards with which products available on the UK market must comply. The policy document lists some areas that may need covering by the legislation, including:

- User authentication
- Vulnerability reporting
- Software updates
- Protection of data at rest and in transit
- Security design principles for software and hardware
- Protection of personal data (privacy)
- Product and wider network resilience
- Provisions of information and guidance to product users

The intended legislation will also enable Ministers to mandate product assurance for particular categories of consumer connected devices. The UK's National Cyber Security Centre already has a Commercial Product Assurance scheme for smart meters, which helps meter makers demonstrate that the security functions of their products meet its standards. This approach could become a model for assurance schemes for other product categories. Three voluntary assurance schemes have already been launched to give shoppers confidence that a smart product has been made cyber secure. They are an Internet of Toys Assurance Scheme, a Smart TV Cybersecurity Certification programme, and the IASME IoT Security Assured initiative that enables start-ups to assess the cyber security of their offerings.

The UK government intends to introduce the legislation "as soon as parliamentary time allows".

United States

In 2020, the US enacted the Internet of Things Cybersecurity Improvement Act. The Act acknowledges the critical importance of cybersecurity to the government and goes on to mandate the publication of guidelines on the appropriate use and management of IoT devices, a review of agency information-security policies relating to the IoT, and the introduction of policies and principles as necessary. The bill mandates the development of guidelines for reporting and sharing information about security vulnerabilities that could affect government agencies. And it says that agencies can't buy or use IoT devices if doing so would prevent compliance with the new standards and guidelines.

In May 2021, President Biden signed an Executive Order to further strengthen the US's cybersecurity and protect federal government networks. The Order, which followed closely on from cybersecurity incidents such as the SolarWinds attack and the Colonial Pipeline incident, calls for better information sharing between the government and private sector on security breaches, updated cybersecurity standards in the federal government, better software supply-chain security, the establishment of a cybersecurity review board and a standard approach to cyber incidents, and better detection of cybersecurity incidents on federal government networks.

Conclusion

The recent flurry of serious cyberattacks has made it clear that cybersecurity is fundamental to national security, not a 'nice-to-have' solution to a minor technical issue that is poorly understood by politicians. The introduction of billions of low-cost IoT devices to the internet has only increased the security challenge. Governments, international standards bodies, industry groups and more are now moving quickly to make IoT implementations more trustworthy. This is being addressed through the development of checklists, guidelines, standards, business processes, certification schemes, and legislation.

All this activity helps to build the sense that IoT networks will soon be much more trustable. What is missing from these approaches is a strong way of knowing that the devices that populate an IoT ecosystem are genuine and still under the control of the people who introduced them to the Internet. This can only be achieved through hardware, by embedding a unique and immutable identifier within a chip in every device whose presence can be used to verify the device's unique identity and set up the secure communications needed to protect it from being suborned. Until this is widely done, IoT security will remain a patchwork rather than whole cloth.

Contact us

For more information please see **www.cryptoquantique.com**
or contact **info@cryptoquantique.com**