IoT Cybersecurity: Regulation Ready

A Landscape Report – Full Version

Contents

Introduction 5
Regulation Impact on IoT Providers 6
Variation 7
Security-Minded and Regulation Ready 7
Regulatory Frameworks At-a-Glance 9
European Union 9
Overview 9
United States 12
Overview 12
United Kingdom 14
Overview 14
Australia 16
Overview 16
Singapore 18
Overview 18
Conclusion 19
A Call to Action 20
Annex A: Scope and Methodology 21
Annex B: Regulation in Action 21
Regulation in Action: My Friend Cayla 21
Regulation in Action: FTC vs D-Link 22
Annex C: European Union 23
CE Marking 23
Manufacturers, Importers, and Distributors 24
Component Parts 24
Testing and Conformance 24
GDPR 25
Controllers and Processors 26
Security and Data Protection by Design 27
International Transfers 27
Network and Information Systems Directive 27
Operators and Providers 28
Incident Response and Reporting 29
Security 29

Annex D: USA 30
Federal Trade Commission Act 30
Product Review 30
Extraterritorial Impact 30
False Advertising 31
Cybersecurity Information Sharing Act 31
Systems Monitoring and Information Security 32
Privacy 32
Information Sharing 32
Children's Online Privacy Protection Act 33
Directed and Knowingly Collecting Children's Data 34
Personal Information and Parental Consent 34
Security of Personal Information 35
Annex E: United Kingdom 35
Data Protection Act 2018 35
Re-identification and Preventing Disclosure 36
Children's Consent 37
Automated Decision-Making 37
Consumer Rights Act 2015 38
Digital Content 38
Quality of Digital Content 39
Processing Facility 40
Damages to Digital Device or Content 40
Digital Economy Act 41
Direct Marketing 41
Internet Infrastructure 41
Dynamic Spectrum Access Services 42
Annex F: Australia 42
Privacy Act 1988 42
Applicability to Small Businesses 43
Cross-Border Disclosure 43
Security of Personal Information 43
Notifiable Data Breach Act 44
Eligible Data Breach 44
Data Breach Statement 44

Competition and Consumer Act 2010 45
Acceptable Quality 45
Repair and Spare Parts 46
Safety Standards 46
Annex G: Singapore 46
Application of English Law Act 46
Energy Conservation Act 48
Regulated Goods and Labelling 48
Energy-Consuming Systems 48
Health Products Act 49
Registered Health Products 49
Defects in Health Products 50
References 51

Introduction

The Internet of Things (IoT) represents a significant opportunity for the global economy, society and business. Yet, if not properly secured it also poses security, safety and privacy threats to information systems, data, and users. The impact of these threats could range from minor inconvenience to serious financial loss or data breach, and negatively affect health and safety or compromise national security. With these concerns in mind, regulators have already taken action and applied sanctions against IoT providers, relying on existing laws.[1] As a result, there is a veritable minefield of issues that suppliers need to be aware of in each jurisdiction. Unfortunately, gaps in legislation, and resulting changes to regulation, usually become apparent only when something goes wrong.

While the IoT market is growing, many perceive consumer[2] adoption to be lagging compared to market potential. This may be the result of a number of factors, such as lack of interoperability and vendor lock-in, relative ease of use [ref 120], (dis)trust [ref 80], and security concerns [ref 58]. Hopes that security-conscious consumers would create a demand for devices with better security features have yet to materialise. Many believe that a fragmented approach to product security and a lack of regulatory standards risk undermining market confidence and stifle market potential.

Security is not a destination, it is a journey which moves and evolves with technology and capabilities. Adopting a security-focused mind set will support IoT product and service providers in mitigating risks ranging from cybersecurity threats to regulatory action. Additionally, technical tools, best practices, and practical steps implemented now may position organisations favourably for future regulatory changes.

Today, some governments and regulatory bodies are applying existing regulation to IoT products and services in an attempt to influence product security and drive user awareness (see Annex B on *Regulation in Action*). Although some may not have been applied to the IoT yet, the regulations analysed in this white paper were found relevant to the IoT in one manner or another. It is also apparent that particular types of existing regulation and their compliance mechanisms are more applicable than others to security-related risks. This is particularly true for regulations such as consumer protection, competition, product marking or labelling, child protection, data protection, cybersecurity, and (tele)communications.

The regulatory landscape around IoT is expected to change significantly in the near future, with unpredictable impacts on innovation and the security of legacy devices. At the time of this report, national or regional level IoT-specific regulation has yet to be enacted. However, governments and regulatory bodies – such as in the EU, US, UK, and Australia – are known to be developing or considering new legislation specific to the IoT.

[1] See the Annex B *Regulation in Action*.

[2] For the purpose of this white paper, "consumer" is interpreted as a person who purchases IoT goods or services for their own use. Nevertheless, many IoT products and services are also applicable to other consumers such as enterprise, governments, or distributors, and are subject to regulation. The paper notes differences where there is a need to specify.

For these reasons, this white paper examines a cross-section of fifteen existing regulations in five jurisdictions (as of September 2018) and explores how these policies may be applied to the IoT. It also considers how IoT products which implement good security practices mitigate regulatory liabilities in the IoT supply chain and create baseline security of IoT technologies. The positive follow-on effects may improve stakeholder confidence and accelerate consumer adoption.

Analysis of these regulations is intended as a resource for IoT manufacturers, innovators, distributors, retailers, and regulatory bodies to better understand the current regulatory landscape and the differences and similarities across jurisdictions. These entities are broadly referenced here as IoT providers and specified by type where needed to capture nuance.

Regulation Impact on IoT Providers

Whether IoT providers are prepared or not, a range of existing regulations could have serious financial and reputational implications for an organisation or individual if found to be non-compliant. A number of factors will influence the type and scope of regulations applicable to an IoT provider. For example, the regulations for regional and national marketplaces, whether the provider is a government supplier or is acting as a third-party provider, the specific product offering including the types of devices and services, and relationship to public or critical resources (e.g. water and fiber networks).

As shown in the *Security-Minded and Regulation Ready* section, adoption of existing tools will help mitigate non-compliance risks. The fifteen policies analysed in this white paper (from the European Union, United Kingdom, USA, Australia and Singapore) highlight the range of applicable regulations, from product marking, to data protection, and competition.[3] Common sanctions for non-compliance with these regulations could have serious financial and reputational implications for corporations and staff, including:

- Fines
- Personal liability and imprisonment of managers or officers
- Cease and desist orders
- Erasure of data
- Public announcements and product recalls
- Binding instructions on security features

The financial sanctions that may be imposed vary by country and type of regulation. Below are examples of maximum fines for non-compliance yet these financial penalties alone are unlikely to represent the full picture as other costs may be incurred such as reimbursement for damages, repair, replacement, refund, and/or audit(s), searches, loss of data, and revocation or re-registration to act in a market.

[3] IoT regulation is a rapidly evolving space at this time. All regulations and analysis are up to date as of September 2018.

Regulation	Maximum Fine[4]
General Data Protection Regulation (EU) [ref 41]	€10 million up to 2% global turnover or, €20 million up to 4% global turnover
Federal Trade Commission Act (USA) [ref 55]	$41,484 (per violation, per day)
Digital Economy Act (UK) [ref 109]	£20,000 a day not to exceed 10% of gross revenue
Privacy Act 1988 and Notifiable Data Breaches Acts (Australia) [ref 16]	A$420,000 (individuals) A$2.1 million (corporations)
Health Products Act (Singapore) [ref 92]	S$50,000 (individuals) S$100,000 (corporations)

Table 1 Financial Penalties

It is difficult to estimate how breach of these regulations might fully impact an IoT provider as a number of factors such as fiscal turnover, financial stability, and even business strategy will affect the result. In addition to financial penalties, providers may lose key personnel or suffer reputational damage which, in turn, may lead to negative effects on sales, share prices, and market trust.

Variation

Existing regulations vary considerably and should be reviewed carefully before entering a new market. For instance, in the UK the age of child consent for information society services[5] is 13, while GDPR sets the age at 16 [ref 105]. Australia, California and EU laws require notification to a supervisory authority in the event of a personal data breach. However, if a breach in Australia warrants notification to the Information Commissioner, the Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) requires organisations to automatically notify individuals as well [ref 10]. This is in contrast to regulations such as GDPR which allows Information Commissioners to assess the need for notification and only explicitly requires notification to "high risk" data subjects [ref 37].

One area where existing general regulation has already had an impact is the toy market. Due to strict child protection laws that lower the barrier for regulatory action, there have been a number of cases brought against smart toys – some resulting in the ban or destruction of the toy.[6] As a result, it was noted by an industry expert consulted in the preparation of this report, that smart toy manufacturers are slowing their introductions to EU and North American markets [ref 62].

Security-Minded and Regulation Ready

From the policy review, it is clear that both technical (e.g. encryption) and organisational tools (e.g. formal policies) should be adopted by companies throughout the lifecycle of a

[4] This only covers penalties due to the relevant body/regulator and does not include any additional financial penalties or payments required by law, such as reimbursement for cost or damages to consumers and court fees.

[5] Information society services in the DPA is defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (Directive (EU) 2015/1535) with the exception of preventative or counselling services.

[6] See Annex B *Regulation in Action: My Friend Cayla*

product, service or system (e.g. security and privacy by design) to demonstrate compliance with relevant legislation.

Actions such as information gathering/logging, data mapping, and internal policies and procedures may support compliance activities, such as cybersecurity certifications or conformity assessments.[7] Many of the controls exist today. Below is a table which reflects some of the technical and organisational tools and resources to help manufacturers mitigate risk.

Organisational Tools & Resources
Vulnerability disclosure/information sharing policy (e.g. communications channels with national CERT/CSIRTs)
Information gathering and reporting mechanisms
Incident response plans
Privacy and security-by-design frameworks
Risk assessment
Data protection/privacy impact assessment
Data protection officer
Information management or data protection policy
Data mapping to understand data flows and access
Clear requirements in consumer and third-party contracts
Ensuring third parties meet adequate policy compliance requirements
Local IoT provider representative (i.e. physical legal presence in geographic area)

Table 2 Organisational Tools and Resources

Technical Tools & Resources
Internationally recognised standards
Certification and conformity assessment (self- and third-party)
Testing (e.g. compliance, penetration tests)
Product lifecycle management and support
Software and firmware update/patch
System monitoring and audit
Traffic monitoring and/or blocking
Maintaining system or technical logs
Alerts (e.g. intrusion detection, abnormal access requests)
Encryption
Pseudonymisation or anonymisation
No use of default passwords

Table 3 Technical Tools and Resources

Certification based on recognised international standards and best practices is one approach that will improve an organisation's 'compliance profile'– both self-certification and independent test-laboratory assessments. This may be developed around national guidance such as the UK Government's Code of Practice for Consumer IoT Security [ref 22] or the USA's NIST Cybersecurity Framework [ref 74] and Privacy Engineering Program [ref

[7] For example, adoption of the IoTSF Security Compliance Framework or expected ENISA cybersecurity certification scheme as part of the forthcoming Cybersecurity Act

75] or using internationally recognised frameworks such as the IoT Security Foundation's (IoTSF) Security Compliance Framework [ref 67].

At the time of publication, it is widely anticipated that reputable IoT providers will adopt, and regulators will support or mandate, compliance frameworks to demonstrate regulatory compliance.

Below is a table of sectors where requirements for security compliance are likely to appear in the near future. Example products included in the table are provided for illustration only and are not based on upcoming regulation.

Sector	Product Examples
Energy	• Smart meters • Solar panels • Large-scale energy management system (e.g. for a business park)
Medical	• Glucose monitors • Vital signs monitor • Connected MRI scanner
Transportation	• After-market E-call solutions • GPS trackers • Driverless cars and components such as autonomous breaking systems
Industrial IoT	• Factory floor robots • Quality control systems • Autonomous machines

Table 4 Projecting Compliance Framework Application

Regulatory Frameworks At-a-Glance

This section provides a brief overview of some existing regulatory frameworks that are relevant to IoT products by a country or region. More information on each jurisdiction and regulation can be found in the corresponding Annex.

European Union

Overview

- CE Marking
- General Data Protection Regulation (GDPR)
- Network and Information Security Directive (NIS Directive)

More detailed information on these regulations can be found in Annex C.

CE Marking ensures the safety, health, and environmental protections of products on the market in the EU [ref 28]. Applicable product categories and regulations may be updated at any time, underlining regulation's shifting landscape[8]. CE marking and associated

[8] See Annex C for a full list of the currently regulated areas.

regulations may have direct impact on both the product (e.g. a device) and organisation depending on the specific regulation.

In addition, product manufacturers, importers and distributors are liable for ensuring compliance with CE Marking – particularly if the device is marketed under their name [ref 33]. In this case, IoT providers will need to obtain the appropriate information from the manufacturer to prove compliance. This may be difficult for distributors if the information is proprietary.

Regulation	Sanctions
CE Marking	• Removal or recall of the product from the EEA marketplace • Penalties • Fines • Imprisonment (The above as laid out in relevant regulation)

Table 5 Sanctions: CE Marking

Regulatory Requirement	Security-Minded Treatment Examples
CE Marking: Importers and Distributors	• Clear requirements and information sharing in third-party contracts • Risk assessment
***The Blue Book*, Section 5: Conformity Testing** "A product is subjected to conformity assessment both during the design and production phase."	• Certification and conformity assessment (self- and third-party) • International standards • Privacy- and security-by-design frameworks

Table 6 Treatment Examples: CE Marking

It is important for IoT providers and their supply chain to be aware of the manner in which the **EU's General Data Protection Regulation (GDPR)** applies to each organisation. Specific application of the regulation can vary by country, so local regulations should be reviewed when entering a marketplace within the EU.

The regulation applies to data controllers and processors acting in the EU marketplace and/or handling personal information of EU residents and citizens. In an IoT environment the body responsible for compliance is likely to be the direct provider, such as a device provider (e.g. smart toy or refrigerator provider), utility provider (e.g. Internet service provider or electricity provider), or digital service provider (e.g. cloud services).

In the IoT environment it is increasingly difficult to draw a line between data controllers and processors and may result in joint or dual designation – this risk is in addition to the increased liability for data processors implemented by GDPR. Data protection regulations are also applicable to product developers and manufacturers involved in the design and development of IoT products but not acting as an IoT provider [refs 38, 40].

While GDPR does not make any specific requirements on technical or organisational security measures for compliance, it does present examples of 'appropriate' safeguards for specific provisions – such as encryption and pseudonymisation. Safeguards are to be determined by the organisation to 'ensure a level of security appropriate to the risk' [ref 39].

Regulation	Sanctions
General Data Protection Regulation	• Fines between 2-4% global turnover, or up to €10-20 million (whichever is greater) • Warnings or orders including erasure of data • Temporary or permanent processing restriction • Communications with data subjects • Suspension of data flows outside the EU or to an international organisation

Table 7 Sanctions: General Data Protection Regulation

Regulatory Requirement	Security-Minded Treatment Examples
Article 25: Data protection by design and default	• Adoption of privacy-by-design and security-by-design frameworks • Implementation of Article 45: Data protection impact assessment • Adoption of self- and third-party assessment schemes • Encryption • Pseudonymisation or anonymisation
Article 32: Security of Processing "resilience of processing systems and services"	• System monitoring and auditing • Testing (e.g. compliance, penetration tests) • Traffic monitoring and/or blocking

Table 8 Treatment Examples: General Data Protection Regulation

The **Network and Information Security Directive (NIS Directive)** applies only to those IoT providers designated as an Operator of Essential Services (OESs) – such as gas, electricity and water – and/or a Designated Service Provider (DSPs). In the IoT ecosystem, OESs are likely to be those providers working in areas like Smart Cities. Most other relevant IoT providers will fall under the DSP heading which includes online marketplaces, search engine, or cloud computing services. As with GDPR, an entity can be designated as both an OES and DSP. In some cases, DSPs have more explicit requirements regarding incident response and reporting [ref 43].

Regulation	Sanctions
Network and Information Security Directive	• Adherence to "binding instructions" from the competent Authority on security • Penalties • Relevant sanctions in national regulation

Table 9 Sanctions: Network and Information Security Directive

Regulatory Requirement	Security-Minded Treatment Examples
Articles 14 & 16: Security requirements and incident notification (OESs & DSPs) (incident notification requirements)	• Maintaining system logs and backup files • Information gathering and reporting mechanisms • Incident response plans
Article 14 & 16: Security requirements and incident notification (OESs & DSPs) "take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems"	• System monitoring and audit • Risk assessment • Third-party audits by the competent authority or a qualified auditor

Table 10 Treatment Examples: Network and Information Security Directive

United States

Overview

- Federal Trade Commission Act (FTC Act)
- Cyber Security Information Sharing Act (CISA)
- Children's Online Privacy Protection Act (COPPA)

More detailed information on these regulations can be found in Annex D.

The **Federal Trade Commission Act (FTC Act)** regulates unlawful and anti-competitive behaviour in the marketplace such as "unfair or deceptive acts or practices" [ref 53]. Examples include failure to take steps to ensure the safety and security of a product and false advertising. There are already a number of cases and warnings the FTC has brought against IoT providers under the FTC Act for reasons of security and safety, ranging from routers and cameras[9] to children's smart watches [ref 56]. In practice, the fines can quickly mount up.[10] As security of IoT products becomes a decision factor for consumers, IoT providers should be able to substantiate their security claims and be clear in intention.

For US-based IoT providers deploying in jurisdictions outside the US, the FTC Act may still apply. If the product has or is likely to cause significant injury to customers – including foreign governments and/or their citizens – the US-based company may be sanctioned, including restitution to foreign victims [ref 52].

Regulation	Sanctions
Federal Trade Commission Act	• Fines up to $41,484 per violation, per day • Restitution for domestic and foreign victims • Audits (one-off or repeated) • Product recall or cease and desist orders • Imprisonment • Federal court and/or state civil action lawsuit • Requests for documentary evidence

Table 11 Sanctions: Federal Trade Commission Act

Regulatory Requirement	Security-Minded Treatment Examples
Section 52: Dissemination of false advertisements (misrepresentation)	• Internationally recognised standards • Certification or conformity assessment • Adoption of security and best practice frameworks
Section 45: Unfair methods of competition unlawful; prevention by Commission (causes or is likely to cause substantial injury)	• Product lifecycle management and support • Encryption • Anonymisation and pseudonymisation
Section 50: Offenses and penalties (failure to produce documentary evidence)	• Certification or conformity assessment • Data Protection Policy • Privacy- and security-by-design policies • System or technical logs or backup files

Table 12 Treatment Examples: Federal Trade Commission Act

[9] See Annex B *Regulation in Action: FTC vs. D-Link*

[10] VIZIO's $2.2 million settlement for unauthorised data collection included a $1.5 payment to the FTC. For more see: https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it

Cyber Security Information Sharing Act (CISA) is a proactive regulation fostering public-private partnerships in cybersecurity information sharing. Unlike other regulations which set strict sanctions for non-compliance, voluntary participation in CISA *relieves* companies of some legal liabilities and offers protections from the Freedom of Information Act [ref 118]. Some of the most stringent requirements in CISA relate to safeguards for personal information associated with incidents and indicators.

Similar to GDPR, CISA provides signposts of acceptable security-minded behaviour for companies and will require technical and organisational capabilities to participate. The government has provided guidance on information that may be classified and shared as "cyber threat indicators" and "defensive measures" [ref 27].

Regulation	Benefits
Cybersecurity Information Sharing Act	• Relief from some legal liabilities • Protection from the Freedom of Information Act

Table 13 Benefits: Cybersecurity Information Sharing Act

Regulatory Requirement	Security-Minded Treatment Examples
Section 5(a): Sharing of cyber threat indicators and countermeasures with the Federal government (Cyber Threat Indicators)	Maintaining system or technical logs and report capabilities including information such as: • Web server log files • IP addresses • Technique allowing unauthorised access • Vulnerabilities found in software • Domain name lookup patterns • Malware • Types of compromised information (per USA Government guidance)
Section 5(a): Sharing of cyber threat indicators and countermeasures with the Federal government (Counter or Defensive Measures)	• Traffic monitoring and/or blocking • Signatures in intrusion detection systems • Firewall rules blocking malicious traffic • Algorithms used to indicate malicious activity • Techniques for scanning SMTP traffic for known threats (per USA Government guidance)

Table 14 Treatment Examples: Cybersecurity Information Sharing Act

Children's Online Privacy Protection Act (COPPA) has already been used to implement strong rules governing the use of children's data and targeting of content [ref 50]. COPPA provides a lower barrier to regulating products, albeit generally child-focused products. The impact of child protection regulation is likely to expand as the IoT environment is increasingly imbedded in households and schools. One difficulty for IoT providers is how and if the provider "knowingly" collects children's data [ref 47] – including third parties such as cloud providers and web services [ref 48].

Regulation	Sanctions
Child Online Privacy Protection Act (Rule)	See sanctions for the FTC Act

Table 15 Sanctions: Child Online Privacy Protection Act (Rule)

Regulatory Requirement	Security-Minded Treatment Examples
"Knowingly" collects children's data	• Data protection policy

(including third parties such as cloud providers and web services)	• Anonymisation or pseudonymisation • Clear requirements in third-party contracts
Section 312.5: Parental consent (option to not consent to sharing data with third-parties)	• Child-focused privacy and data impact assessment • Data mapping to understand data flows and access • Anonymisation or pseudonymisation

Table 16 Treatment Examples: Child Online Privacy Protection Act (Rule)

United Kingdom

Overview

- Data Protection Act 2018 (DPA)
- Consumer Rights Act 2015 (CRA)
- Digital Economy Act (DEA)

More detailed information on these regulations can be found in Annex E.

The **Data Protection Act 2018 (DPA)** is the UK's primary data protection legislation and implements GDPR at the local level [ref 107]. It is important to note, some articles of GDPR allow national governments leeway in implementation, so IoT providers should review local legislation. Among other provisions, requirements related to automated decision-making are outlined in the DPA to protect the subject's rights from decisions with legal or "significant" impact [ref 104]. This may be particularly relevant to IoT providers as it is common for IoT products and services to offer automation as one of many value-adds for consumers or the providers' business model.

Regulation	Sanctions
Data Protection Act 2018	• Notices • Powers of entry (searches) • Penalties or fines (see GDPR) • Data being forfeited, destroyed or erased • Directors or managers held personally liable

Table 17 Sanctions: Data Protection Act 2018

Regulatory Requirement	Security-Minded Treatment Examples
Section 170: Unlawful obtaining etc of personal data **Section 171. Re-identification of de-identified personal data**	• Compliance with the ICO's Data Sharing Code of Practice • Clear requirements in consumer and third-party contracts • Data protection policy • Anonymisation and pseudonymisation
Section 14: Automated decision-making authorised by law: safeguards	• Maintaining system or technical logs or backup files • Data protection or privacy impact assessment • Information security and management policy

Table 18 Treatment Examples: Data Protection Act 2018

Updates to the **Consumer Rights Act 2015 (CRA)** in 2015 included a new section on consumer rights regarding digital content which is particularly relevant to IoT providers. Digital content is broadly defined as "data which are produced and supplied in digital form" and must be of "satisfactory quality" [ref 97].

The provisions highlight the importance of lifecycle management – including after-market product support. Providers with a security mind set will understand the need to be prepared for future risks and incidents. IoT providers may also be liable for damages caused to or by consumers' digital device resulting from the provider's less than quality digital content – for example, malware [ref 100]. IoT providers should protect their systems from incoming threats and take measures to protect or verify outward flows of data to avoid liability for down-stream issues.

Regulation	Sanctions
Consumer Rights Act 2015	• Fines • Cost such as for damages, repair, replacement or refund • Termination of contracts • Investigations • As applicable from other regulations such as Enterprise Act 2002

Table 19 Sanctions: Consumer Rights Act 2015

Regulatory Requirement	Security-Minded Treatment Examples
Section 34, Digital content to be of satisfactory quality (fit for purpose, free of minor defects, safe, durable)	• Product lifecycle management and support • Encryption • Software and firmware update/patch • Internationally recognised standards
Section 46(1): Remedy for damage to device or to other digital content	• Traffic monitoring and/or blocking • Software and firmware update/patch • Firewalls and gateways • Verification of data

Table 20 Treatment Examples: Consumer Rights Act 2015

The **Digital Economy Act (DEA)** is different from the other UK Acts included in this report in that it both sets new provisions, for instance with reference to internet filters, and modifies other existing Acts, such as the Communications Act [ref 109].

Not all IoT providers will be significantly affected by the DEA, but instead providers of specific types of IoT products or services. For instance, there are provisions regarding digital infrastructure including elements of 5G which may be relevant for ISPs as well as IoT providers that manage networks or access to the internet or online content [ref 108]. IoT providers in the gas and electric, and water and sewerage sectors will be subject to information sharing and processing requirements [ref 103], and IoT devices which may be at risk of or are intended to receive marketing materials and spam may be subject to additional requirements [ref 106].

Regulation	Sanctions
Digital Economy Act	• Fines (e.g. £20,000 a day not to exceed 10% of gross revenue) • Notices • Imprisonment (up to 2 years) • As applicable from other regulations such as Privacy and Electronic Communications Regulations and Direct Marketing Code

Table 21 Sanctions: Digital Economy Act

Regulatory Requirement	Security-Minded Treatment Examples
Chapter 1: Public service delivery (disclosure of information)	• Data protection/privacy impact assessment • Anonymisation or pseudonymisation • Clear requirements in third-party contracts • Data protection policy

Table 22 Treatment Examples: Digital Economy Act

Australia

Overview

- Privacy Act 1988
- Notifiable Data Breach Act (NDB Act)
- Competition and Consumer Act 2010 (CCA)

More detailed information on these regulations can be found in Annex F.

The **Privacy Act** sets out 13 Australian Privacy Principles (APPs) applicable to local and extraterritorial companies processing personal information [ref 9]. Principles particularly relevant to IoT providers include topics such as anonymity and pseudonymity, use or disclosure of personal information, cross-border disclosure of personal information, and security of personal information.

In the case of cross-border transfers, the local provider is also responsible for ensuring the extra-territorial entity is not in breach of the APPs [ref 7]. Should a third party experience a data breach the local provider will need to execute an impact assessment to determine if a local data breach notification is required.

Regulation	Sanctions
Privacy Act 1988 and **Notifiable Data Breaches Act 2017**	• Orders • Enforceable undertakings • Penalties • Compensation • Personal fines up to A$420,000 • Corporate fines up to A$2.1 million

Table 23 Sanctions: Privacy Act 1988

Regulatory Requirement	Security-Minded Treatment Examples
APP 8: Cross-border disclosure of personal information	• Clear requirements in third-party contracts • Risk assessment • Data protection/privacy impact assessment
APP 11: Security of personal information (unlawful access, disclosure, or loss of personal information)	• Role-based access control • Pseudonymisation or anonymisation • Encryption • Maintaining system or technical logs

Table 24 Treatment Examples: Privacy Act 1988

The **Privacy Amendment (Notifiable Data Breaches) Act (NDB Act)** requires companies to submit a data breach notification to the Australian Office of the Information Commissioner within 30 days of becoming aware of a breach that is likely to result in serious harm to the individual [ref 13].

In addition, the company is automatically required to notify affected individuals or provide a public statement on the event for *all* notifiable data breaches [ref 12]. The public notification requirements are stricter than those seen in other data protection regulations such as GDPR which only requires data subject notification in "high risk" situations [ref 37].

Regulation	Sanctions
Privacy Amendment (Notifiable Data Breaches) Act 2017	See sanctions for the Privacy Act 1998

Table 25 Sanctions: Privacy Amendment (Notifiable Data Breaches) Act 2017

Regulatory Requirement	Security-Minded Treatment Examples
Section 26WK: Statement about eligible data breach	• Maintaining system or technical logs • Data mapping to understand data flows and access • Incident response plans • Data protection policy

Table 26 Treatment Examples: Privacy Amendment (Notifiable Data Breaches) Act 2017

The **Competition and Consumer Act 2010 (CCA)** regulates a variety of market factors including anti-competitive practices and consumer law [ref 6]. Products must be fit for purpose, free from defects and safe [ref 2]. For example, the protection of personal information using encryption may support product safety or quality. Information and system security measures like software patch and updates may support protection from defects.

An aspect of assessing "quality goods" includes review of statements and labelling by the provider on the IoT product and packaging [ref 3]. During the lifecycle of the product, there is a guarantee to the consumer for repairs and spare parts for a "reasonable" period of time after purchase, which may be supported by IoT product lifecycle management [ref 5].

Regulation	Sanctions
Competition and Consumer Act 2010	• Compensation for losses • Reimbursement • Disqualifying and individual from managing a corporation • Injunctions • Safety warnings or recalls • Corporate penalties up to A$1.1 million • Non-corporate penalties up to A$220,000

Table 27 Sanctions: Competition and Consumer Act 2010

Regulatory Requirement	Security-Minded Treatment Examples
Volume 3, Schedule 2, Section 54: Guarantees as to acceptable quality and	• Product lifecycle management • Software and firmware update/patch • Internationally recognised standards
Volume 3, Schedule 2, Section 55: Guarantees as to fitness for any disclosed purpose, etc	• Certifications or conformity assessments • Privacy and security-by-design frameworks • Internationally recognised standards and best practices
Volume 3, Schedule 2, Section 58: Guarantees as to repairs and spare parts	• Lifecycle management • Software and firmware update/patch • Clear requirements in consumer contracts and terms of service

Table 28 Treatment Examples: Competition and Consumer Act 2010

Singapore

Overview

- Application of English Law Act (AELA)
- Energy Conservation Act (ECA)
- Health Products Act (HPA)

More detailed information on these regulations can be found in Annex G.

The original **Application of English Law Act (AELA)** was enacted in 1993. Its purpose is to clarify the "extent to which English law is applicable in Singapore", as well as any updates to existing laws [ref 86]. It has since been through two updates, with the most recent version active as of March 2012. The laws most applicable to IoT providers are commercial law. The Insurance Act [ref 83], Supply of Goods and Services Act [ref 84], and Unfair Contract Terms Act [ref 85], all have amendments included in the AELA text. A reference table of these and other applicable laws can be found in Annex G.

Regulation	Sanctions
Application of English Law Act	• As per the relevant English law

Table 29 Sanctions: Application of English Law Act

Regulations	Security-Minded Treatment Examples
Insurance Act **Supply of Goods and Services Act Unfair Contract Terms Act**	• Clear requirements in consumer and third-party contracts • Internationally recognised standards • Certification and conformity assessment

Table 30 Treatment Examples: Application of English Law Act

The **Energy Conservation Act (ECA)** sets out requirements for energy management and conservation practices [ref 90]. This regulation may be applicable to any IoT product requiring electricity or fuel, is interconnected with at least one other good, and they are interdependent or interact. If a system does not meet the required energy efficiency, then the provider is responsible for maintenance or other measures to ensure the system meets the standards [ref 88]. This may result in significant cost to an IoT provider in retrofitting deployed systems.

Regulation	Sanctions
Energy Conservation Act	• Fine up to S$10,000 • Cost incurred for meeting energy efficiency standards

Table 31 Sanctions: Energy Conservation Act

Regulatory Requirement	Security-Minded Treatment Examples
Section 26B(2): Minimum energy efficiency standards for energy-consuming systems	• Internationally recognised standards • Certification and conformity assessments • System monitoring and audit • Traffic monitoring and/or blocking

Table 32 Treatment Examples: Energy Conservation Act

The **Health Products Act (HPA)** regulates the manufacture, import, supply, storage, presentation and advertisement of health-related products [ref 93]. All products and

manufacturers, importers or wholesalers must be registered with the Authority. Relevant IoT products may include medical robots, implants such as glucose monitors or pace makers, temporary and portable medical devices as well as “cosmetic devices” such as toothbrushes or water picks, laser hair removal devices, UV patch, or hair brushes.

If the registrant of a health product becomes aware of a “defect” or an “adverse effect” from the product it must be reported to the Authority. The definition of a "defect" is broad and could encompass a number of IoT-related risks for health devices [ref 91]. For instance, if a health device is found not to be “patchable” after a vulnerability discovery, the product may being deemed of "inadequate quality" and taken out of service or off the market.

Regulation	Sanctions
Health Products Act	• Product recalls • Public statements • Personal fines up to S$50,000 • Corporate finds up to S$100,000 • 2 years imprisonment

Table 33 Sanctions: Health Products Act

Regulatory Requirement	Security-Minded Treatment Examples
Section 42(2): Reporting of defects and adverse effects to Authority	• Product lifecycle support • Software and firmware update/patch • Vulnerability disclosure policy
Section 15: Prohibition against supply of unregistered health products	• Certification and conformity assessment • Internationally recognised standards • Testing (e.g. compliance, penetration tests)

Table 34 Treatment Examples: Health Products Act

Conclusion

At the time of publication, IoT-specific regulation has yet to be enacted. Currently, many governments are cautious to implement legislation that may be perceived as negatively impacting innovation, deployment and entrepreneurship. Yet some, like South Korea, have taken an alternative approach by rolling back potentially restrictive regulation to facilitate the adoption of the IoT and other technologies [ref 121]. With cybersecurity being of concern to governments, citizens, industry and consumers, further regulation in the IoT ecosystem is highly likely.

Some national regulatory regimes are in development and review stages – such as the US IoT Cybersecurity Improvement Act and EU Cybersecurity Act [refs 35, 117]. However, others have only hinted at ideas for future regulation. For instance, Australia is reportedly assessing a consumer rating system for IoT products [ref 18].

Jurisdiction	Regulation or Policy	Status
European Union (EU)	EU Cybersecurity Act (Regulation) [ref 35]	Trialogue final text negotiations
USA	Internet of Things (IoT) Cybersecurity Improvement Act [ref 117]	Introduced in the Senate
California	Security of Connected	Effective 1 January 2020

(USA)	Devices Act [ref 70]	
UK	Code of Practice for Consumer IoT Security [ref 22]	The UK has signposted the Code of Practice as a base of future regulatory action [ref 67]. It builds on the government's Security by Design Report which is currently going through the standardisation process in the European Technical Standards Institute (ETSI).
Australia	Consumer IoT rating system	Proposed
Singapore	Focus on open standards [ref 94]	In the National strategy

Table 35 Regulation in Development

A Call to Action

Industry needs to be proactive and not only adopt a security-focused mind set to adapt to an evolving regulatory landscape and global marketplace, but also communicate clearly that it is doing so. This security-focused mind set should, at minimum, take into consideration the design, production, operation, tools and lifecycle processes of IoT products and services. This will support regulatory compliance, demonstrate due diligence and a duty of care, and reduce risks of non-compliance. Adopting this approach also enhances baseline security of IoT products and services in the marketplace and can help protect against risks associated with some legacy devices.

It is critical for IoT providers to factor in additional resources and procedures for product lifecycle support. As IoT security is a journey, not a destination, companies should be prepared to support their products for the duration of this journey. Implementation of security best practices, such as the ability to update and patch, and adopting known good schema, such as IoTSF's Security Compliance Framework, will not only sustain resistance to cyber-attacks, it will also assist in regulatory compliance and mitigate corporate liabilities. The ability to support claims related to good security practices and regulatory compliance may improve consumers' trust and confidence in IoT products and services and encourage further adoption of IoT products and solutions.

This white paper only scratches the surface of exiting regulation that applies to the evolving IoT marketplace and is not intended to be a comprehensive overview of applicable law and regulation. It has not reviewed, for example, national implementation of the EU's Network and Information Systems Directive. However, there are also a variety of guidelines and resources (formal and draft) published by governments that may assist with local compliance activities, such as:

- EU's ENISA Baseline Security Recommendations for IoT [ref 36]
- USA's NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (draft guidance) [ref 57]
- UK's Code of Practice for Consumer IoT [ref 22]
- Australia's Guide to Data Analytics and the Australian Privacy Principles [ref 77]
- Singapore's Guidelines for IoT security for smart nation [ref 82]

Annex A: Scope and Methodology

This regulatory policy review focused on aspects of the regulations most applicable to the IoT environment, or unique manners of influencing that environment. This may include actions that should be taken by the organisation or design features that may impact an IoT product. For instance, the UK Consumer Rights Act analysis focuses on the section regarding "digital content" and does not go into detail of other sections such as goods and consumer contracts which are generally applicable to market goods.

It is generally understood that the regulations apply within the relevant jurisdiction. Cases of extraterritorial reach (e.g. Australian Privacy Act or GDPR and cross-border data flows) have been included where particularly relevant.

In this paper the term "IoT product" is used to represent the devices, services and other aspects of the IoT in the marketplace.

Five jurisdictions were chosen for this study to reflect diversity in regions and regulatory structures as well as reflect a variety of legislation, innovative approaches to and fostering growth in IoT and regulation. Those five jurisdictions are:

- European Union
- United Kingdom
- United States of America
- Australia
- Singapore

A cross section of digital-focused and traditional legislation was chosen for review from these five jurisdictions. These included regulations in areas such as:

- Critical infrastructure
- Data protection
- Consumer protection and trade regulations
- Child online protection
- Electric goods
- Health products
- Incident disclosure/information sharing

Annex B: Regulation in Action

Regulation in Action: My Friend Cayla

My Friend Cayla is a smart toy that can interact with children by using speech recognition to process language and respond as if in conversation. On the outside, the toy seems harmless enough. However, by 2015 a number of consumer rights groups, pentesters and governments began reviewing the technology behind My Friend Cayla. It took another two years for regulatory action.

Concerns regarding the security and privacy of the doll resulted in it being pulled from some shelves in Germany and requesting the doll to be destroyed by parents. The German

Bundesnetzagentur (or Federal Network Agency) classified the toy as a "concealed surveillance device" under the German Telecommunications Act and found the wireless connection was not "adequately protected" [ref 17]. Reportedly, some Dutch shop owners refunded parents, even though the toy had not been recalled in the Netherlands [ref 21].

Prior to this ruling, entities in least three other countries had flagged the dangers posed by My Friend Cayla. In 2015 Pen Test Partners, a UK-based company, reported a security vulnerability that allowed someone to hack the toy [ref 15]. In 2016 the Norwegian Consumer Council issued a review of the toy to BEUC (the European Consumer Organisation) noting user terms breaching the EU's Unfair Contract Terms Directive, EU Data Protection Directive, and child protection regulation [ref 95]. Concurrently, in the USA a group of consumer and digital rights groups filed a formal complaint with the Federal Trade Commission based on lack of compliance with the Child Online Privacy Protection Act and Federal Trade Commission Act [ref 20].

Many of the initial actions were taken by consumer rights groups, with complaints working up to national and regional governments. Furthermore, a result of having child protection acts and specific data protection requirements for children's products meant a lower barrier for regulatory action. For My Friend Cayla it was less a case of whether or not the toy would come under fire from governments or regulators, and much more a case of the most efficient legislative process to take action.

Regulation in Action: FTC vs D-Link

In 2017 the FTC took D-Link Systems, Inc., a Taiwan-based company and its US subsidiary, to court over its internet cameras and routers on the grounds of unfairness and misrepresentation outlined in the FTC Act. The FTC claimed D-Link "failed to implement proper security safeguards." This left devices vulnerable to attack and put consumer's privacy at risk, including audio/video feeds and login credentials [ref 54]. This is not the first time D-Link has come under fire for security flaws. In 2013 an obvious back door was found in router software [ref 69].

Although the case was ultimately dismissed, three of the six accounts brought against D-Link were found plausible. These include misrepresentation of information regarding security including event response, router security, and IP camera protection from unauthorized access and control.

Promotional materials claiming "easy to secure" and "advanced network security" were not backed up by the devices' technical capabilities or the company's business practices. For instance, the FTC found D-Link used hard coded login credentials (i.e. "guest" for username and password) for the camera, had a known software flaw in the router, left sensitive information openly available online (i.e. the private key code for D-Link software), and left users' login credentials in clear text (unencrypted) on their mobile devices [ref 54].

The FTC's claim that D-Link engaged in unfair business practices likely to cause "substantial injury to consumers" [ref 51] was not upheld by the judge. However, the case was lost almost on a technicality, with the judge proposing that if the FTC had taken another

approach to the unfairness claim – one that focused on the collective impact of a small security flaw on a large number of people instead of "actual consumer injury" such as monetary loss, the exposure or misuse of sensitive personal data – there may have been a different outcome to the case [ref 19].

Annex C: European Union

CE Marking

CE Marking indicates product conformance with harmonised European directives and regulations on the safety, health and environmental protections of products [ref 28]. Because CE Marking relates to the product, requirements for obtaining the mark may have direct impact on both the organisation and the product, such as an IoT device or supporting third party cloud solution. CE Marking is required for all devices in relevant product categories on the market in the EEA, including devices created and/or produced outside the Union [ref 28], used, second-hand, and modified products [ref 32]. Conversely, products that do not fall under the purview of a relevant product category may *not* acquire a CE Marking.

Product categories and relevant regulations can be updated at any time. Additionally, if an IoT product falls under more than one category (e.g. machinery and construction products), then it must prove conformance with all relevant categories [ref 32]. The current product categories are [ref 34]:

- Active implantable medical devices
- Appliances burning gaseous fuels
- Cableway installations designed to carry persons
- Construction products
- Eco-design of energy related products
- Electromagnetic compatibility
- Equipment and protective systems intended for use in potentially explosive atmospheres
- Explosives for civil uses
- Hot-water boilers
- In vitro diagnostic medical devices
- Lifts
- Low voltage
- Machinery
- Measuring instruments
- Medical devices
- Noise emission in the environment
- Non-automatic weighing instruments
- Personal protective equipment
- Pressure equipment
- Pyrotechnics
- Radio equipment

- Recreational craft
- Restriction of hazardous substances in electrical and electronic equipment
- Safety of toys
- Simple pressure vessels

Member States are required to sanction manufacturers, importers or distributors for failure to comply with CE Marking requirements. In addition to removal and recall of the product from the EEA marketplace, these may include penalties and/or criminal sanctions such as fines and imprisonment [ref 32].

Manufacturers, Importers, and Distributors

Normally, manufacturers are responsible for proving conformance for CE Marking. However, where an importer or distributer markets the device under their own name, they assume legal responsibility for the CE Marking [ref 33]. This means that if, for example, an energy provider or internet service provider (ISP) acquire a third-party device (e.g. smart meter or router) for distribution in the EEA under their brand, the energy provider or ISP will be responsible for the CE Marking as well as holding sufficient information on the design and production of the product to support conformance with the mark.

Component Parts

IoT products may include component parts which fall under the purview of CE Marking. For example, a smart water heater may fall under the categories of *appliances burning gaseous fuels* as well as *radio equipment* for components used to connect to mobile networks or broadband. In such cases, both the component part (in this case radio equipment) and the smart water heater would need to bear CE Marking [ref 32][11].

Testing and Conformance

Some products can be self-assessed by the manufacturer. However, others may require conformance assessment by a Notified Body. A notified body is an "organisation designated by an EU country to assess the conformity of certain products before being placed on the market." [ref 31]. Each country within the EU will have designated Notified Bodies [ref 30] which oversee third party conformance assessment procedures. These bodies can carry out a variety of tasks such as testing (within and outside the country) and information sharing with notifying authorities, surveillance authorities, or other notified bodies. Providers should do a thorough check and review of the required conformance procedures for their product.

Compliance frameworks include both the design and production phase.[12] Regulations will specify when a Notified Body is required in order to satisfy conformity provisions. While currently no "security by design" or similar IoT security framework language is specifically referenced in the compliance frameworks, it is probable that regulations will be updated to formalise security risk assessments and audits when relevant European or international standards are recognised.

[11] [ref 32] Section 4.5.1.6.
[12] [ref 32] Section 5.1.1.

For example, the new Radio Equipment Directive (RED) requires a Notified Body for audit and numbering on the product label. It also requires ongoing compliance and audits, which may be an appropriate approach in an evolving security landscape. Extending existing conformance requirements in Directives like RED could seamlessly integrate good security principles or practices into the conformity test for IoT products which fall under the Directive.

Additionally, inclusion of these measures may serve to prove compliance with other existing EU regulations when required. GDPR is one such regulation which stipulates "Data protection by design and by default" and includes certification mechanisms as a compliance method.[13] Until such compliance methods are fully functional, it is suggested that manufacturers adopt guidance, such as the UK's *Secure By Design Report* [ref 110] and IoTSF Security Compliance Framework [ref 67] during IoT product design and production phases to support compliance with relevant harmonised standards.

GDPR

The EU's General Data Protection Regulation (GDPR) is arguably the most comprehensive data protection policy to date [ref 42]. It makes data controllers and processors liable for data protection and management. The Regulation sets out seven key principles, these are [ref 66]:

- Lawfulness, fairness and transparency (e.g. data breach notification and preventing client lock-in)
- Data minimisation (e.g. only collecting data needed to deliver the product)
- Purpose limitation (e.g. only processing the data for its intended purposes)
- Accuracy (e.g. the ability to correct inaccurate information)
- Storage limitation (e.g. duration and state of data retention)
- Integrity and confidentiality (security) (e.g. Security by design, encryption, pseudonymisation)
- Accountability (e.g. fines, Data Protection Impact Assessment)

Non-compliance with GDPR can result in a variety of sanctions with resounding impact on the organisation's reputation and ability to continue business, including:

- Warnings or orders including erasure of data
- Temporary or permanent processing restriction
- Communications with data subjects
- Suspension of data flows outside the EU or to an international organisation
- Fines

Fines associated for non-compliance vary depending on the type of infraction.[14] For instance, a fine of up to €10 million or 2% worldwide annual turnover may be imposed on data controllers and processors for infractions related to children's consent, data protection by design and default, processing records, and breach notification.

[13] [ref 42] Article 25:
[14] [ref 42] Article 83: General conditions for imposing administrative fines.

Larger fines of up to €20 million or up to 4% worldwide annual turnover may be imposed on data controllers and processors for infractions related to processing, consent, data subject rights, and non-compliant international transfer.

Although we have yet to see how effective such a comprehensive approach to data protection may be, the risk mitigation and compliance mechanisms associated with GDPR largely reflect those applicable to other types of regulations included in this report. In addition to newer compliance requirements such as designation of a local representative and data protection officer, more traditional compliance mechanisms include:

- Data Protection Impact Assessment[15]
- Clear contracting terms[16]
- Adoption of international standards and best practices[17,18]
- Self- and third-party certification schemes[19]
- Technical best practices and state-of-the art solutions[20]
- User consent mechanisms[21]

Controllers and Processors

In IoT environments it may be difficult to identify controllers and processors. Additionally, manufacturers of IoT products may be considered a data controller when applying GDPR. The Regulation defines a controller as the body that "determines the purposes and means" of processing personal data, while a data processor "processes personal data on behalf of the controller".[22]

If a processor or manufacturer has any control or influence over the means or purpose for processing, they may be liable as a joint data controller.[23] For instance, if a cloud computing company is acting as a data processor for a Smart TV provider, but they jointly determine the data that should be collected, algorithms for analysis, and information derived from the process then the cloud computing company may be considered a data controller.

Contracting terms between parties in IoT environments become an important aspect of protection for companies – both as controllers and processors. Contracts should clarify aspects such as the expectations and limits of processing, requirements for other sub-contracted parties, types of data – particularly if personal or sensitive – being processed and expected security measures.

[15] [ref 42] Article 35: Data protection impact assessment.
[16] [ref 42] Article 26: Joint controllers.
[17] [ref 42] Article 43: Certification bodies.
[18] [ref 42] Article 70: Tasks of the Board.
[19] [ref 42] Article 35: Data protection impact assessment.
[20] [ref 42] Article 25: Data protection by design and default.
[21] [ref 42] Article 7: Conditions for consent; and Article 8: Conditions applicable to child's consent in relation to information society services.
[22] [ref 42] Article 4: Definitions.
[23] [ref 42] Article 26: Joint controllers.

Security and Data Protection by Design

In order to support data protection principles such as accessibility, data minimisation, purpose and storage limitation and security principles[24] such as confidentiality, integrity, availability and resilience, GDPR requires data controllers to consider data protection throughout the lifecycle of the product or data protection by design and default.[25] As a result, developers and manufacturers which are not the IoT provider may be considered data controllers. This is based on the widely accepted notion that the manner in which systems, algorithms, and technologies are developed impact the manner in which they are implemented, often having real-world effects (such as locking doors or managing electricity supply) and process personal data.

Therefore, all actors in the IoT supply chain should be aware of how GDPR applies to them and ensure they are compliant, including device manufacturers and data processors who are not the IoT provider. With regard to information security and principles such as data protection by design, tools for compliance may be both technical and organisational and should be appropriate to the assessed risk.

For instance, technical solutions such as pseudonymisation, encryption, and system monitoring and auditing may be adopted to ensure confidentiality, integrity, availability, and resilience of IoT device, services and systems. Internal policies and procedures such as a data breach plan, risk assessments, user privilege management, adoption of the Data Protection Impact Assessment[26] [ref 29] or appointing a Data Protection Officer[27] may also assist when demonstrating compliance.

International Transfers

Transfers to international organisations or countries outside the EEA must meet an adequacy decision by the European Commission, meaning that all parties must comply with GDPR or provide equivalent protections to European residents.[28]

IoT providers within the EEA transferring data to parties outside the region should ensure those parties have met the adequacy requirement. IoT providers – including controllers and processors – not based in Europe will need to designate a local representative in at least one of its countries of operation.[29] This is an important compliance requirement and additional business expense for organisations to factor in.

Network and Information Systems Directive

The Network and Information Systems (NIS) Directive [ref 45] is not likely to have a significant impact IoT devices but may impact the organisations providing direct or third-party services. A number of provisions in the Directive are subject to Member State

[24] [ref 42] Article 32: Security of processing.
[25] [ref 42] Article 25: Data protection by design and default.
[26] [ref 42] Article 35: Data protection impact assessment.
[27] [ref 42] Section 4: Data protection officer.
[28] [ref 42] Chapter 5: Transfers of personal data to third countries or international organisations.
[29] [ref 42] Article 27: Representatives of controllers or processors not established in the Union.

interpretation and therefore may vary between national regulations, such as the definition of "operator of essential services". Additionally, micro and small enterprises[30] should be aware that they are not subject to the requirements in *Chapter V*: *Security of the Network and Information Systems of Digital Service Providers*.[31] Failure to comply with the NIS Directive may result in penalties including "binding instructions" on security set by the Competent Authority.[32]

Operators and Providers

The Directive applies to two groups of service providers, operators of essential services (OESs) and digital service providers (DSPs). OESs can be a public or private entity in a range of national critical infrastructure sectors, particularly:

- Energy
- Transport
- Banking
- Health
- Drinking water supply and distribution
- Digital infrastructure

Designation as an OES is specific to Member States and depends on a variety of criteria including[33]:

- If an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- The provision of that service depends on network and information systems; and
- An incident would have significant disruptive effects on the provision of that service.

IoT providers designated as an OES will likely be those working closely with Smart City deployments or in public utility sectors.

IoT providers not operating in national critical infrastructure sectors are more likely to be designated a DSP. A DSP is any legal person that provides one of the following types of digital services[34]:

- Online marketplace (e.g. potentially a connected refrigerator that makes automated orders)
- Online search engine (e.g. potentially a connected home assistant)
- Cloud computing service (e.g. potentially a home IoT management service)

It is possible for an entity to be designated both an OES and DSP and therefore will need to comply with the requirements of both types of service providers. In an IoT environment, the probability of dual designation is increased. For example, a top level domain (TLD) registry

[30] As defined in Commission Recommendation 2003/361/EC, which sets out requirements for upper bounds for number of employee, as well as an annual turnover not exceeding EUR 50 million and/or annual balance sheet total not exceeding EUR 43 million
[31] [ref 45] Article 16(11)
[32] [ref 45] Article 15: Implementation and enforcement.
[33] [ref 45] Article 6(1)
[34] [ref 45] Article 4(6) and Annex III

may also offer value-add services such as cloud computing service for home IoT management, which may therefore result in dual designation if the registry meets requirements such as number of users, geographic area of impact, and market share.

Incident Response and Reporting

The designation of OESs and DSPs impact the responsibilities of organisations when responding to security incidents. In the Directive, requirements for DSPs are, in some cases, more explicate than for OESs. For instance, additional parameters are specified to assess the scale of an incident affecting a DSP. Both OESs and DSPs are required to consider and report on the number of affected users, duration and geographical area of the incident. DSPs must also report "the extent of the disruption of the functioning of the service" and "the extent of the impact on economic and societal activities".[35]

The collection of relevant data, monitoring of systems, data mapping, and incident response plans are good practices for an organisation to have in place in order to facilitate compliant incident response. In addition, DSPs are required to designate a local representative in at least one Member State where services are offered if the DSP is located outside the European Union.[36]

Security

The articles on security of networks and information systems focus on risk, impact and incident management. OESs and DSPs must “take appropriate and proportionate” measures to manage risks[37], prevent and minimise incident impact.[38]

OESs and DSPs should therefore take the necessary organisational and technical measures to demonstrate compliance with the Directive and national legislation, such as:

- Use of certification schemes
- Adoption of European and internationally recognised standards
- Proof of compliance with standards
- Adoption of state-of-the-art network and information security solutions
- Business Impact Assessment
- Business Continuity Plan, including testing
- Incident Response or Disaster Recovery Plan, including testing
- Monitoring, auditing and testing of systems
- Documented security policies
- Third party audits "by the competent authority or a qualified auditor"[39]

[35] [ref 45] Article 16(4): Security of the network and information systems of digital service providers
[36] [ref 45] Article 18(2)
[37] [ref 45] Article 14(1): Security requirements and incident notification; and Article 16(1): Security of the network and information systems of digital service providers
[38] [ref 45] Article 14(2) and Article 16(2)
[39] [ref 45] Article 15(2) and Article 16(2)

Annex D: USA

Federal Trade Commission Act

The Federal Trade Commission Act (FTC Act) [ref 53] is a broad act that oversees unlawful and anti-competitive behaviour, including “unfair or deceptive acts or practices in or affecting commerce” in the marketplace – including IoT products.[40] An act can also be unlawful and unfair if it is found "likely to cause substantial injury to customers which is not reasonably avoidable."[41] Although no concrete definitions or examples of “unfair or deceptive acts” are included in the document, this may include actions such as failure to take appropriate design and implementation steps to ensure the safety and security of the product, false advertising, and preventing customer product review.

Sanctions for non-compliance with the FTC Act are broad and not particularly specific. These include:

- Formal and informal hearings
- Federal court and/or state civil action lawsuit
- Cease and desist orders
- Fines
- Requests for documentary evidence
- Imprisonment
- Restitution for domestic and foreign victims
- Publication of report findings

It is hard to say what the total impact on a company might be for non-compliance with the FTC Act, but it may range from fines ($41,484 per infraction, per day) to significant reputational, market and financial losses. Some cases against IoT providers have resulted in being subject to series of audits over a 20-year period [ref 46]

Product Review

The sale, lease, or supply of a product cannot prevent a consumer or parties from publicly reviewing a product through contract or other means.[42] As a result, testing or certification centres, penetration testers, individuals, academics, and customers can analyse a product and post a public review. There are already a number of cases where people have tested and then publicised security flaws in IoT devices [refs 59, 99]. The publicity of significant security flaws can damage the reputation of the product and/or the IoT provider as well as the financial stability of the company.

Extraterritorial Impact

Unfair or deceptive acts which are conducted within the FTC’s jurisdiction fall within the scope of the FTC Act. For instance, if an IoT water sensor provider manages its product from

[40] [ref 53] Section 45(a1): Unfair methods of competition unlawful; prevention by Commission.
[41] [ref 53] Section 45(n): Unfair methods of competition unlawful; prevention by Commission.
[42] [ref 53] Section 45b(b(1)): Consumer review protection.

US soil but deploys in both the US and foreign countries, it may be at risk of further investigation under the FTC Act should there be an incident causing or likely to cause significant injury to any of the consumers (possibly foreign governments and/or their citizens).[43] In such a case, the FTC reserves the right to any remedy, including restitution to foreign victims.

False Advertising

False advertising (disseminating or causing to be disseminated) is considered an unfair or deceptive act by the FTC Act.[44] As security of IoT products becomes a factor in purchase decisions for some consumers, claims by IoT providers about their products should be supported. IoT providers claiming to include particular features (e.g. secure communications or encrypted data), compliance with particular certifications schemes or standards, or adoption of security best practices should be able to substantiate their claims to demonstrate compliance with the FTC Act.

To determine if an act is unlawful, unfair or deceptive, the FTC will take into account other public policies, such as the Safe Web Act of 2006 [ref 122]. While the FTC cannot specify any trade rule, regulation or standard to prove compliance, adoption of internationally recognised standards supports compliance with the FTC Act.[45] This may also help the IoT provider support advertising claims, best practices in terms of consumer safety or IoT product security, and the ability to produce documentary evidence. The failure to produce requested documentary evidence may be punished with a fine or imprisonment.[46]

Documentary evidence may include documents, papers, correspondence, books of account, and financial and corporate records.[47] To prove the safety and security of a product or system, in addition to the documents mentioned above, IoT providers may consider documentation of privacy and security by design practices, internal policies and procedures such as privacy policies, business continuity plans, and incident response plans, and technical logs including information such as updates/patches, IoT device lifecycle management or system tests.

Cybersecurity Information Sharing Act

Public-private partnerships in cybersecurity information sharing is widely considered a best practice. The Cybersecurity Information Sharing Act (CISA) constructs a framework of “dos and don’ts” to enable this partnership and two-way information flow [ref 119]. This approach is proactive in enforcing good security practices compared to other more traditional regulations heavily reliant on sanctions for non-compliance. CISA provides authorisation for monitoring systems and implementing defensive measures, as well as protections for participating organisations – particularly from the Freedom of Information

[43] [ref 53] Section 45(a(4(A-B))): Unfair methods of competition unlawful; prevention by Commission.
[44] [ref 53] Section 52(a-b): Dissemination of false advertisements.
[45] [ref 53] Section 57a(a(1(B))): Unfair or deceptive acts or practices rulemaking proceedings.
[46] [ref 53] Section 50: Offenses and penalties.
[47] [ref 53] Section 44: Definitions.

Act[48] and legal liability[49] – and sets out expectations on the type of information classified as "cyber threat indicators" and "defensive measures".

Systems Monitoring and Information Security

CISA authorises information and system monitoring for "cybersecurity purposes", including information in transit, storage, or being processed.[50] This authorisation supports the gathering of information which may then be shared with Federal and private entities under CISA. Additionally, organisations monitoring information systems, implementing countermeasures, or participating in cyber threat information sharing must use security controls "to protect against unauthorised access or acquisition of such cyber threat indicators or countermeasures."[51] The Act does not specify what these methods may be, but adoption of best practices, state of the art technologies or cybersecurity certification schemes may help to ensure compliance.

Privacy

Organisations opting into CISA will need to implement safeguards for indicators – both shared and retained – containing personal information in order to protect privacy and civil liberties. These safeguards should protect from unauthorised access or acquisition and limit the receipt, retention, use and sharing of indicators with personal information.[52] However, personal information related to perpetrators – such as IP and email addresses – may be shared. Organisations will also need an internal process for destruction of information not directly related to identifying or countering an attack and set limits on the duration of time an indicator may be retained. Both policies (e.g. Information Management or Data Protection Policies) and technical tools (e.g. pseudonymisation) may be useful in complying with requirements of privacy of personal and identifiable information.

Information Sharing

CISA authorizes the sharing of cyber threat indicators and countermeasures (or, defensive measures). To comply, organisations will need the capability to share indicators with Federal bodies in real time, or, when not possible, to be shared without undue delay.[53] Internal processes and procedures should be set up in order to ensure the required information can be gathered and shared in a timely manner.

CISA defines a "cyber threat indicator" as "information that is necessary to indicate, describe, or identify" a variety of security incidents, including[54]:

- Malicious reconnaissance
- Exploiting vulnerabilities or overcoming security controls
- A security vulnerability
- Causing unwitting unauthorised access or exploitation

[48] [ref 119] Section 5(d): Information shared with or provided to the federal government.
[49] [ref 119] Section 6: Protection from liability.
[50] [ref 119] Section 4(a): Authorisation for monitoring.
[51] [ref 119] Section 4(d): Protection and use of information.
[52] [ref 119] Section 5(b): Privacy and Civil Liberties.
[53] [ref 119] Section 5(a): Sharing of cyber threat indicators and countermeasures with the Federal government.
[54] [ref 119] Section 2: Definitions.

- Malicious command and control
- Actual or potential harm

Published guidance provides examples of indicators, such as [ref 27]:

- Web server log files
- IP addresses
- Discovery of technique allowing unauthorised access
- Vulnerabilities found in software
- Domain name lookup patterns
- Malware
- Types of compromised information

CISA defines "countermeasure" as "action, device, procedure, technique, or other measure" used to mitigate threats or security vulnerabilities to information systems or information that is stored, processed or in transit.

The same published guidance provides examples of countermeasures that may be shared [ref 27]:

- Programs to identify malicious activity or web traffic
- Signatures in intrusion detection systems
- Firewall rules blocking malicious traffic
- Algorithms used to indicate malicious activity
- Techniques for scanning SMTP traffic for known threats

CISA does not impart strict rules or sanctions for non-compliance as it is a voluntary public-private partnership. But it does provide guidance on the types of information that are useful in identifying and defending a cybersecurity threat, as well as indicate where an organisation may implement both policy/procedure and technical tools to support cybersecurity. As a result, companies wishing to participate in CISA will need to ensure they have the technical and organisational capabilities to gather and share the required information in a timely manner.

Children's Online Privacy Protection Act

Updates to the Children's Online Privacy Protection Act (COPPA) took effect in 2013. It also resulted in an update to the Children's Online Privacy Protection Rule (the Rule) implemented by the FTC and explored here [ref 50]. This included changes to the definition of "personal information" and "collects/collection", provisions on parental consent and rights of the parent to review content. Sanctions for non-compliance with the FTC COPPA Rule are set out in the FTC Act (see the section on the FTC Act).

Directed and Knowingly Collecting Children's Data

The Rule applies to any entity operating an online service directed at or knowingly collecting, using, or disclosing children's data[55], including third parties such as cloud service providers or web support services.[56] Furthermore, the IoT provider must "give the parent the option to consent to the collection and use of the child's personal information without consenting to disclosure of his or her personal information to third parties."[57]

In a connected environment which is increasingly imbedded in families and households, the reach of this regulation is likely expanding, particularly as some ambiguities of application exist. One example is the extent to which an IoT provider will "knowingly" collect children's data [ref 124]. For instance, if a home assistant requests information about the occupants it is fairly straight forward as to whether the IoT provider will "knowingly" be collecting children's data.

However, if a home assistant uses speech recognition and interaction patterns to create user profiles and modify content, then it may be creating children's profiles. The question is to what extent this is "knowingly" done and how safeguards should be put in place for automated data processing, for example implementing alerts based on recognised patterns. An IoT provider may consider an alert system based on account activity. Or, they may consider a more intensive user set-up process to facilitate parental consent. COPPA also requires that parents are able to *not* consent to the transfer of data to third parties. Additionally, systems of systems in IoT environments, clear contracting with consumers and third-party service providers is good practice for compliance with the COPPA Rule.

Personal Information and Parental Consent

One of the updates to the Rule in 2013 is a new definition of "personal information". In this context, personal information now includes[58]:

- Name, address, Social Security Number, and telephone number
- Online contact information
- Screen or user name
- Persistent identifiers
- Geolocation
- Photograph, video or audio file
- Other collected information used to identify the child or parents

Many IoT devices, toys included, are "headless" in that they do not provide an easy to use or comprehensive user interface. This complicates the requirement of verifiable parental consent for those collecting children's data.[59] The Rule does provide some examples of how parental consent may be obtained, which may be useful in a constrained IoT environment –

[55] [ref 50] Section 312.3: Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.
[56] [ref 50] Section 312.2: Definitions
[57] [ref 50] Section 312.5(2): Parental consent
[58] [ref 50] Section 312.2: Definitions
[59] [ref 50] Section 312.5: Parental consent

such as mail-in forms, toll-free numbers, and monetary transactions – and providers should factor appropriate mechanisms into their business models.

An IoT provider should execute a child-focused privacy impact assessment to understand how their product may impact children and requirements for use of their personal information. Additionally, COPPA provides parents the right to review personal information collected by the website.[60] In this case, it is also useful to have a data map and customer engagement strategy to support appropriate responses for when this information is requested.

Security of Personal Information

COPPA requires that confidentiality, integrity, and security of personal information is maintained using "reasonable procedures" and only shared with third parties who also possess these capabilities and can provide assurances to that effect.[61] This includes stricter data retention and deletion policies than are standard for personal information of adults in the US.

Entities are required to delete personal information after the retention has passed what is "reasonably necessary to fulfil the purpose for which it was collected"[62]. Notably, this does not include a caveat to retain anonymised data like some privacy acts governing the use of adults' data. An information management and security policy including data retention policy may be useful in proving compliance with these provisions. Additionally, the base language is reflective of the "CIA" approach to information security – confidentiality, integrity, and availability – suggesting that best practices, state of the art technologies, and international standards in this area would be acceptable measures to implement.

Annex E: United Kingdom

Data Protection Act 2018

The UK's Data Protection Act 2018 (DPA) [ref 107] updates the previous 1998 Act and incorporates the relevant requirements set out in the EU's GDPR.[63] In addition, the Information Commissioner's Office (ICO) is setting out guidance and DCMS have published fact sheets for the DPA on the topics of:

- General processing [ref 23]
- Law enforcement processing [ref 24]
- Intelligence services processing [ref 25]
- Information Commissioner and enforcement [ref 26]

[60] [ref 50] Section 312.6: Right of parent to review personal information provided by a child.
[61] [ref 50] Section 312.8: Confidentiality, security and integrity of personal information collected from children.
[62] [ref 50] Section 312.10: Data retention and deletion
[63] As the DPA translated GDPR into national legislation, this section does not focus on translated requirements such as the equivalency requirement for transfer of data outside the EU, or rights to erasure, rectification or restriction of processing.

This section focuses on requirements set out by the UK in those four areas and the DPA's application to IoT products. In particular:

- Criminal offenses related to unlawful obtaining, re-identification and alteration to prevent disclosure of personal data
- Children's age of consent
- Safeguards related to automated decision-making

The *Enforcement* section of the DPA sets out the variety of notices, powers of entry, penalties, appeals, etc. granted under the act.[64] Additionally, it lists specific offenses relating to personal data for which corporate body directors or managers may be held liable in addition to other sanctions.[65] Criminal offences may result in fines, data being forfeited, destroyed or erased – which can have a variety of implications for IoT providers reliant on data for their businesses, ranging from the negative effects of a financial burden to downsizing or even closure.[66]

Re-identification and Preventing Disclosure

The DPA makes re-identification and processing of such data without the controller's consent a criminal offense.[67] Another offense makes the obtaining, retaining, disclosing, or procuring disclosure of personal data without consent of the data controller a criminal offence.[68] It is also criminal to alter, deface, block, erase, destroy or conceal data to which the data subject otherwise has rightful access.[69]

In an IoT environment it may be particularly difficult to identify data controllers, processors, and unauthorised processors – particularly if many devices supplied by different providers and third-party solutions are communicating data between them. This increases the risk that a data processor may breach the DPA through re-identification, processing or disclosing information without the controller's consent.

To mitigate risks related to unauthorised processing or blocking of access, data controllers and processors can ensure compliance with the ICO's soon to be updated code of practice on sharing data[70], data controllers may consider using tools such as data mapping. A data map provides an overview of information such as the personal data an organisation holds, where it is stored, where it came from, how/from whom it was obtained, who is responsible for that data, and how it is being processed. Additional tools such as information audits and contract review can be used to assist data mapping.

[64] [ref 107] Part 6: Enforcement.
[65] [ref 107] Section 198. Liability of directors etc
[66] [ref 107] Section 196(3). Penalties for Offenses
[67] [ref 107] Section 171. Re-identification of de-identified personal data
[68] [ref 107] Section 170: Unlawful obtaining etc of personal data.
[69] [ref 107] Section 173: Alteration etc of personal data to prevent disclosure to data subject.
[70] [ref 107] Section 121. Data-sharing code

Children's Consent

One key difference between the GDPR and DPA is the lower age limit for a child's consent when accessing 'information society services'.[71] The UK's DPA sets the age limit for information society services consent at 13[72] while GDPR sets this age limit at 16.[73] IoT providers will need to ensure that they are compliant with the age of consent rules, particularly in obtaining parental consent for the collection, processing, and storing of personal information. For the safeguarding of children online, ensure that relevant age verification and content management tools, including techniques such as strong data protection and de-identification, are implemented appropriately.

Automated Decision-Making

Particulars pertaining to the safeguards of automated decision-making and its potentially significant impacts are set out in the DPA. Automatic decision-making is particularly relevant for IoT products, some of which provide quicker processing and more automated real-world impact than previously experienced. For instance, this section may be relevant to auto insurance providers whose customers have a data recorder in their car. In the case where an automatic decision is made which impacts the premium or coverage of a customer may result in that customer not having insurance or having a different level of coverage. In turn, this may result in significant impact upon the individual, particularly in the event of an incident.

For those implementing automated decision-making using personal information, there must be mechanisms set up to protect the subject's rights, freedoms and legitimate interests, particularly if resulting in a "significant decision" which results in legal or similarly significant affects to the data subject.[74] To do this, the DPA requires those taking decisions solely based on automated processing to[75]:

- Notify the data subject as soon as possible
- Allow the data subject one month to provide additional information, request a review of the decision, and non-automated processing of a decision
- Respond to the data subject within a month of the steps taken and outcome of the request after complying the request and any considering additional information provided by the data subject

To mitigate the risks associated with automated decision-making, IoT providers should have formal processes set up in alignment with the DPA for notifying data subjects, receiving and reviewing requests from the data subject, and responding to the data subject, including steps taken to comply with the request and any outcome from the request. The provider

[71] Information society services in the DPA is defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (Directive (EU) 2015/1535) with the exception of preventative or counselling services.
[72] [ref 107] Section 9: Child's consent in relation to information society services
[73] [ref 42] Article 8(1): Lawfulness of processing: public interest etc.
[74] [ref 107] Section 14(1-2): Automated decision-making authorised by law: safeguards
[75] [ref 107] Sections 14(4-5): Automated decision-making authorised by law: safeguards

will also need a manner of logging and tracking information about how the decisions are made and clearly communicating this to the data subject.

Consumer Rights Act 2015

The UK Government updated the Consumer Rights Act (CRA) in 2015 [ref 101]. This included two new sections on consumer rights regarding digital content (data), and ability to provide reasonable care and skill [ref 123]. Updates were made in unfair contract terms, faulty goods, uncompetitive behaviour, notice for routine inspections, and flexibility in responding to breaches in consumer law. This section focuses on those elements of the CRA most applicable to IoT products and overall environment security, in particular the chapter on Digital Content.

An IoT provider's failure to comply with the provisions set out for Digital Content specifically, can result in consumers exercising a variety of their rights, including but not limited to[76]:

- Right to reject
- Right to repair or replacement
- Right to price adjustment
- Final right to reject or end of contract
- Claim damages
- Seek specific performance
- Seek order for specific implementation
- Reimbursement or refund, including for costs incurred

The potential financial and reputational risks of non-compliance are significant, ranging from £5,000 to cost such as for damages, repair, replacement or refund. To mitigate the risks associated with these sanctions, IoT providers may consider a variety of treatments.

Digital Content

In the CRA, "digital content" is defined as "data which are produced and supplied in digital form".[77] Therefore, digital content is not "online content" in the terms of images, voice, video or text. This broad definition of digital content is thereby applicable to IoT products, as are the regulations set out in the CRA. Section 39 on *Supply transmission and facilities for continued transmission* in particular acknowledges various business models by which data, devices, and service providers interact, nodding to the IoT marketplace.

The IoT marketplace is supported by a variety of business models. The CRA generally applies to goods and services paid for by money (or supplied in conjunction with other paid goods, services or content) and does not necessarily include services which are "free".[78] The CRA

[76] [ref 101] Section 19(3,9,11), Consumer's rights to enforce terms about goods; and Section 42, Consumer's rights to enforce terms about digital content.
[77] [ref 101] Section 2(9): Key definitions.
[78] [ref 101] Section 33: Contracts covered by this Chapter.

therefore does not apply to free access through models such as unpaid “free-mium” access or products that are “paid for” by exchanging data unless the digital content causes damage, in which case liability *cannot* be excluded or restricted.[79]

The CRA sets out recommendations as well as requirements for the contracting of goods and services, many of which are applicable to IoT products by virtue of being on the marketplace[80], while others are more specific to digital content[81] and service contracts.[82] Failure to include particular information in a contract, such as specifications on fit for purpose digital content, may result in breach of contract and liability of the company.

Quality of Digital Content

An important aspect of the digital content provisions focuses on the “quality” of the digital content, or data.[83] Failure to provide “quality” digital content (i.e. fit for purpose, free of minor defects, safe and durable content) related goods and services – in particular “processing facilities” – for anything less than a "reasonable time" would be a breach of the CRA. “Processing facilities” are how the IoT provider receives data from and transmits data to the consumer. Presumably this could include communications technologies, services (e.g. cloud computing or user interfaces), devices, hardware and software.

The state and condition of the data will be assessed on at least 4 points:

- Fit for purpose
- Free of minor defects
- Safety
- Durability

This opens the door to a variety of ways in which an IoT provider may be in breach of contract when supplying digital content. For example, if personally identifiable or other sensitive data is transferred unencrypted, this may not comply with the "safety" requirement. Likewise, unsecured data in transit is at risk of a man in the middle attack which may impact the “durability” (interpreted here as integrity) of the data.

If known vulnerabilities are found in the digital content or if digital content is compliant with flawed or out of date standards this may be failure to provide data "free of minor defects". If electricity notifications based on National Grid capacity are time delayed in distribution to IoT products preventing them from optimising energy capacity this may not be "fit for purpose". Therefore, providers should ensure customer contracts include all the necessary information relevant to quality of digital content, in particular its purpose, even if it is a common application to avoid being in breach of contract.[84]

[79] [ref 101] Section 47: Liability that cannot be excluded or restricted.
[80] [ref 101] Chapter 2: Goods.
[81] [ref 101] Chapter 3: Digital content.
[82] [ref 101] Chapter 4: Services.
[83] [ref 101] Section 34: Digital content to be of satisfactory quality.
[84] [ref 101] Section 35(3), Digital content to be fit for a particular purpose.

Processing Facility

Section 39 references data flows between IoT provider, the consumer, and devices and "processing facilities". A processing facility is how the IoT provider receives data from and transmits data to the consumer.[85] Presumably, this could include communications technologies, services (e.g. cloud computing or user interfaces), devices, hardware and software.

Unless otherwise specified in the contract, it is required that the processing facility be made available to the consumer for a "reasonable time".[86] This provision can be used to protect consumers from early end-of-life and end-of-service provisioning or planned obsolescence. Issues like this have already come up in the US, such as Google Nest's decision to brick the Revolv home device [ref 60]. Like cybersecurity, IoT product support is not a destination, it is a journey. IoT product support should be provided for the lifecycle of the product and factored into the design and business plan.

From discussion with industry, it is apparent that may IoT providers, particularly SMEs, are not aware of the ongoing cost for supporting deployed IoT products or services, particularly with relation to cybersecurity [ref 61]. IoT providers should build into their project plans and business models IoT product support for the lifecycle of the product. Failure to provide less than "quality" digital content (i.e. fit for purpose and free of minor defects), related goods and services for anything less than a "reasonable time" would be in breach of the CRA.

Damages to Digital Device or Content

The IoT provider may also be liable for damages caused to the consumer's digital device or other digital content by data supplied by the provider and "would not have occurred if the trader had exercised reasonable care and skill."[87] For instance, if providers do not implement appropriate security tools or good practices for traffic monitoring or blocking of suspicious packages, malware or other viruses may be sent from the provider to consumer devices, corrupting data, rendering the device unusable, and possibly causing more serious harm resulting from the malfunction or stoppage of an IoT product. In this case, the IoT provider may be liable for damages caused by the digital content (i.e. malware) and be required to repair or compensate the consumer for damages.

Considering the large scale of some deployments (e.g. business parks or manufacturing plants), the cost associated with non-compliance may be significant for IoT providers and risk the financial standing and/or public opinion of the company. It is important that appropriate care is taken to protection incoming and outgoing data. If incoming data is not monitored or verified, compromised data may be transferred to IoT provider systems from customer devices which may not be deployed in particularly secure environments. The IoT provider could then potentially transfer on corrupted data or viruses to other customers. Providers should also take measures to protect outward flows of data to ensure that compromised or malicious data does not cause down-stream issues which the company may be liable for.

[85] [ref 101] Section 39(4), Supply by transmission and facilities for continued transmission.
[86] [ref 101] Section 39(5), Supply by transmission and facilities for continued transmission.
[87] [ref 101] Section 46(1): Remedy for damage to device or to other digital content.

Digital Economy Act

The Digital Economy Act 2017 (DEA) is different from the other UK Acts included in this report in that it both sets new provisions – for instance with reference to internet filters – and modifies other existing Acts – such as the Communications Act – some of which have since been updated (e.g. Data Protection Act 1998 and 2018) [ref 109].

Not all IoT providers will be significantly affected by the DEA, but instead providers of specific types of IoT products or services. For instance, there are provisions regarding digital infrastructure including elements of 5G which may be relevant for ISPs as well as IoT providers that manage networks or internet access.[88] Solutions that provide access to online content will be subject to provisions on internet filtering[89] as well as access to pornographic[90] and "seriously harmful extrinsic material".[91] IoT providers in the gas and electric, and water and sewerage sectors will be subject to information sharing and processing requirements.[92] And IoT devices which may be at risk of or are intended to receive marketing materials and spam – such as smart refrigerators or home assistants – may need to comply with the DPA, the Privacy and Electronic Communications Regulations on direct marketing and follow the Direct Marketing Code.[93]

Direct Marketing

The Information Commissioner's Direct Marketing Code (the Code) was recently updated to comply with GDPR [ref 64]. The Code includes advice on email and online marketing, which may be interpreted to include communications to IoT products. General rules apply, such as consent for direct marketing, "soft opt-in" for existing customers, and the right to opt-out. The right to opt-out must be supported and may pose difficulties for direct marketing materials sent to devices without user interfaces or are operated by voice command to opt out or find information on how to opt out of advertising. Online marketing that is not "targeted" (i.e. sent to every user or based on content rather than personal information) is generally not covered by the DPA, but direct marketing is.

Internet Infrastructure

IoT products and services providing internet access or making up components of that infrastructure will need to comply with a variety of policies regarding universal access and the Electronic Communications Code, including the DEA, Communications Act 2003 and Telecommunications Act 1984. The DEA also modifies the Communications Act, changing the terminology "conduit" to "infrastructure" and "conduit system" to "system of infrastructure", thereby making those IoT providers supplying or managing such infrastructure subject to the Electronic Communications Code.[94]

[88] [ref 109] Part 1: Access to digital services; and Part 2: Digital Infrastructure.
[89] [ref 109] Section 104: Internet filters.
[90] [ref 109] Part 3: Online Pornography; particularly Sections 14 and 19
[91] [ref 109] Section 92: Digital additional services: seriously harmful extrinsic material.
[92] [ref 109] Part 5: Chapter 1: Public service delivery.
[93] [ref 109] Section 96: Direct marketing.
[94] [ref 109] Section 4: The electronic communications code

Dynamic Spectrum Access Services

Requirements for dynamic spectrum access (a technology used in 5G) service providers are also included in the DEA and makes amendments to the Wireless Telegraphy Act 2006.[95] A dynamic spectrum access service is a service that provides information about[96]:

- the availability for use by wireless telegraphy stations and wireless telegraphy apparatus of frequencies that fall within a frequency band specified in regulations made by OFCOM, and
- the places in which, the power at which, the times when and any conditions subject to which such stations and apparatus may use such frequencies.

Organisations providing dynamic spectrum access services "may be registered" by OFCOM.[97] OFCOM also has the right to revoke registration[98] which, in addition to penalties up to £20,000 a day or 10% of "relevant amount of gross revenue"[99] may prevent IoT providers from supplying services, including testing.

Annex F: Australia

Privacy Act 1988

The Privacy Act 1988 [ref 9] is the overarching data protection legislation in Australia and sets out the 13 Australian Privacy Principles (APPs) [ref 78], including principles such as:

- Anonymity and pseudonymity
- Use or disclosure of personal information
- Cross-border disclosure of personal information
- Security of personal information

Sanctions for non-compliance fall into three categories:

- Determinations
- Penalties
- Enforceable undertakings

Determinations and enforceable undertakings can vary from requirements to take or cease actions, orders to prevent an action from occurring, or compensation for infractions.[100] Penalties[101] for individuals can be up to A$420,000, while corporations face a maximum of A$2.1 million [ref 16]. The APPs, applicability requirements and sanctions set out in the Privacy Act also apply to Australia's new Notifiable Data Breaches Act (see next section).

[95] [ref 109] Section 8: Regulation of dynamic spectrum access services.
[96] [ref 109] Section 8(1), Part 2A (53A[7])
[97] [ref 109] Section 8(1), Part 2A (53A): Registration of providers of dynamic spectrum access services.
[98] [ref 109] Section 8(1), Part 2A (53B): Revocation and variation of registration.
[99] [ref 109] Section 8(1), Part 2A (53F): Penalties under section 53E.
[100] [ref 9] Section 33: Commissioner may except undertakings; and Section 52: Determination of the Commissioner.
[101] [ref 9] Part VIB: Civil penalty orders.

Applicability to Small Businesses

The Privacy and Notifiable Data Breach Acts apply to small businesses[102] differently than larger organisations. However, it is likely that many small business IoT providers will be subject to the Acts. Small businesses that provides health services, hold health information, disclose personal information for benefit, provide a service collecting personal data, or is a contracted provider for a Commonwealth contract are all subject to the Acts.[103] Therefore, it is important for relevant small IoT providers operating in Australia to ensure they can comply with the Privacy Act, including appropriate technical and policy safeguards for personal information.

Cross-Border Disclosure

IoT systems regularly cross borders, for example via a multinational provider, cloud services, or other third-party contractors. The Privacy Act does not prevent the use of extraterritorial providers for data collection, processing, and service delivery, however the provider does need to comply with the APPs.[104] It is the responsibility of the organisation liable to the Privacy Act (for instance the local IoT service provider) to ensure "the overseas recipient does not breach" the APPs.[105] The only instance when a known breach of the APPs may not result in action by the Commissioner is if the action is required by local law of the overseas party.[106] Should the overseas party experience a breach, the responsible organisation will need to execute an impact assessment to determine if a data breach notification is required. In these instances, it is important to ensure there are clear contracts between providers in place, including expectations of data privacy and security and data breach impact assessment and response plan are in place.

Security of Personal Information

APP 11 requires organisations to secure personal information from misuse, interference, loss, unauthorised access, modification or disclosure.[107] Additionally, organisations must take steps to destroy or de-identify personal information that is no longer needed.[108] Specific technical or policy solutions for meeting these requirements are not provided in the Act. However, adopting best practices, guidance documents, and international standards is an effective way to ensure compliance. For instance, privilege management and technical tools such as firewalls can protect information from misuse and unauthorised access. It is also apparent that organisations should have an information management strategy, including time scales and policies on data destruction/de-identification.

[102] A small business is one with an annual turnover of A$3 million or less. Privacy Act, Section 6D: Small Business and small business operators
[103] [ref 9] Section 6D: Small business and small business operators.
[104] [ref 78] APP 8: Cross-border disclosure of personal information.
[105] [ref 78] APP 8: Cross-border disclosure of personal information.
[106] [ref 9] Section 6A: Breach of an Australian privacy principle
[107] [ref 78] APP 11: Security of personal information.
[108] [ref 78] APP 11: Security of personal information.

Notifiable Data Breach Act

The Privacy Amendment (Notifiable Data Breaches) Act 2017 (NDB Act) sets requirements for notifying the Office of the Australian Information Commissioner (OAIC) in the case of an eligible data breach [ref 13]. Applicability and sanctions can be found in the Privacy Act 1988 (see above). In addition, organisations are required to notify affected individuals or provide public statements on the organisation's website, or other by reasonable steps to publicise the information as determined by the Commissioner.[109] This required step of public notification upon notification to the Commissioner not seen in other acts such as GDPR may increase the reputational impact to a company as a result of a data breach.

In order to comply with the public notification requirement, organisations may find it useful to have internal policies on incident response and escalation (including data breach), data breach notification, and outreach strategies.

Eligible Data Breach

An eligible data breach is the unlawful access, disclosure, or loss of personal information likely to result in serious harm to the individual.[110] If a data breach occurs or is suspected, organisations must complete their assessment within 30 days of becoming aware of the breach.[111] There is a wide variety of information that should be considered when assessing if a data breach is likely to cause serious harm. Some are related to system and information security, for example[112]:

- The kind or kinds of information breached
- The sensitivity of the information
- Whether the information is protected by one or more security measures
- If the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome
- And in the case of technologies like encryption, have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology

In order to comply with the NBD Act, and identify the likelihood of serious harm resulting from a data breach, an organisation should have well documented information such as data mapping, privacy impact assessments, escalation policies, and security strategies.

Data Breach Statement

Organisations who experience, or suspect to have experienced, an eligible data breach must supply a statement to the Information Commissioner. In order to comply with the data breach statement requirements, the organisation will need to provide description of the

[109] [ref 13] Section 26WR: Commissioner may direct entity to notify eligible data breach.
[110] [ref 13] Section 26WA: Notification of eligible data breaches
[111] [ref 13] Section 26WH: Assessment of suspected eligible data breach.
[112] [ref 13] Section 26WG: Whether access or disclosure would be likely, or would not be likely, to result in serious harm—relevant matters

data breach and the type(s) of data involved.[113] In order to provide a suitable data breach notification, an organisation should be able to rely on internal resources such as data mapping and information management policies, system monitoring, audits and access logs.

Competition and Consumer Act 2010

The Competition and Consumer Act 2010 [ref 6] covers a wide variety of subject matter, sectors, and requirements, including [ref 14]:

- Third party access to nationally significant essential facilities
- Accesses to services for telecommunications
- Anti-competitive practices, enforcement and remedies
- Consumer law

Schedule 2 focuses on consumer law regarding goods and services, including safety and information, country of origin representations, labelling, and information standards.[114] Failure to comply with the provisions set out by the CCA may result in a number of sanctions for the organisation or individual, including[115]:

- Reimbursement of financial benefit "obtained directly or indirectly"
- Compensation for losses, damages and/or to victims
- Public warning about the conduct of a person or corporate body (adverse publicity order)
- Disqualifying an individual from managing a corporation
- Injunctions
- Recalls
- Safety warnings
- Pecuniary penalties

Maximum pecuniary penalties can range from A$5,000 to A$1.1 million for corporate bodies and A$1,000 to A$220,000 for non-corporate bodies depending on the action. Failure to comply with the CAA may result in a broad range of sanctions for both individuals and corporations found in breach of the act.

Acceptable Quality

Goods and services must be fit for purpose; goods must also be free from defects and safe – in addition to other provisions – in order to comply with the CCA.[116] These principles may be applied to IoT product security.

Likewise, if a product is disclosed to have a particular purpose (such as provide secure and private video surveillance), then any product found not supporting the disclosed purpose is

[113] [ref 13] Section 26WK: Statement about eligible data breach.
[114] [ref 6] Volume 3, Schedule 2: Consumer Law
[115] [ref 6] Volume 3, Schedule 2, Chapter 5: Enforcement and remedies
[116] [ref 6] Volume 3, Schedule 2, Section 54: Guarantees as to acceptable quality; and Section 61: Guarantees as to the fitness for particular purpose, etc.

in breach of the CCA.[117] IoT providers may consider using certifications and best practice frameworks to in order to support the claims or representations made about a product.

Repair and Spare Parts

In the sale of goods, there is a guarantee to the consumer for repairs and spare parts for a reasonable period of time after purchase.[118] This may be interpreted in such a way that it is applicable to IoT product lifecycle management. For example, should a device no longer work properly due to changes in the system - such as implementation of new or migration to different connectivity technologies. IoT providers should ensure that they are able to support their products for a "reasonable" period of time, or that they make explicit in the contract the duration of time that parts and facilities for repair will be available to consumers.

Safety Standards

Safety[119] and information[120] standards can be made for goods and services at any time. Safety standards can be enforced using an international standard, a part of a standard, or a national standard by Standards Australia. Failure to comply with standards requirements may result in a temporary or permanent ban on the product.

Safety standards for goods may include provisions on aspects such as the performance, manufacture, design, or construction of the product. Safety standards for services may include the manner and method of supply, materials used to supply the service, and testing of the service.

Standards may also be placed on the information which is provided along with an IoT product, such markings (e.g. labels), warning, or instructions. This may include provisions on content, specific information to be included or excluded, and the manner or form by which it is provided.

Annex G: Singapore

Application of English Law Act

The application of English laws most relevant to IoT providers are commercial laws – predominantly applicable by virtue of acting in the marketplace or being a corporate body rather than technical specificity [ref 86]. Below is a reference table of the applicable laws.

[117] [ref 6] Volume 3, Schedule 2, Section 55: Guarantees as to fitness for any disclosed purpose, etc.
[118] [ref 6] Volume 3, Schedule 2, Section 58: Guarantees as to repairs and spare parts.
[119] [ref 6] Volume 3, Schedule 2, Section 104: Making safety standards for consumer goods and product related services.
[120] [ref 6] Volume 3, Schedule 2, Section 143: Making information standards for goods and services.

Act[121]	Overview	Updates
Partnership Act 1890 [ref 113]	An Act to declare and amend the Law of Partnership. Partnership is the relation which subsists between persons carrying on a business in common with a view of profit.	The whole act.
Third Parties (Rights against Insurers) Act 1930 [ref 76]	An Act to make provision about the rights of third parties against insurers of liabilities to third parties in the case where the insured is insolvent, and in certain other cases.	The whole except the amendments effected by the Insolvency Act 1985 and the Insolvency Act 1986.
Corporate Bodies' Contracts Act 1960 [ref 102]	An Act to amend the law governing the making of contracts by or on behalf of bodies corporate; and for connected purposes.	The whole act.
Misrepresentation Act 1967 [ref 112]	An Act to amend the law relating to innocent misrepresentations and to amend sections 11 and 35 of the Sale of Goods Act 1893.	The whole act.
Unfair Contract Terms Act 1977 [ref 116]	An Act to impose further limits on the extent to which under the law of England and Wales and Northern Ireland civil liability for breach of contract, of for negligence or other breach of duty, can be avoided by means of contract terms and otherwise, and under the law of Scotland civil liability can be avoided by means of contract terms.	Part I (except section 1(1)(c) and (3)(b) and the amendment to that section by the Occupiers' Liability Act 1984) and Part III.
Sale of Goods Act [ref 114]	An Act to consolidate the law relating to the sale of goods.	The whole except sections 22 and 25(2).
Supply of Goods and Services Act 1982 [ref 115]	An Act to amend the law with respect to the terms to be implied in certain contracts for the transfer of the property in goods, in certain contracts for	The whole except Part II.

[121] [ref 86] First Schedule, Part II: Enactments relating to commercial law.

	the hire of goods and in certain contracts for the supply of a service; and for connected purposes.	
The Insurance Act [ref 111]	An Act to make new provision about insurance contracts; to amend the Third Parties (Rights against Insurers) Act 2010 in relation to the insured persons to whom that Act applies; and for connected purposes.	See AELA text

Table 36 Singapore: Application of English law act

Energy Conservation Act

The Energy Conservation Act (ECA) mandates the requirements for complying with energy management practices with the aim of energy conservation, efficiency and reduction of environmental impact [ref 90]. Goods relevant to this Act include any device, appliance, equipment, article or thing that requires electricity or fuel, is interconnected with at least one other good, and they are interdependent or interact. Prohibited supply of regulated goods that do not meet these standards or non-compliance with the Act may result in a fine up to S$10,000.

Regulated Goods and Labelling

Regulated goods that use energy must meet the minimum energy efficiency standard and be labelled with the required information.[122] Information regarding minimum energy efficiency standards can be found on the National Environment Agency's (NEA) website [ref 71]. Regulated goods encompass a variety of devices and sectors, including white goods (e.g. refrigerators and clothes driers), entertainment equipment (e.g. televisions), and other household goods (air conditioners and lamps) [ref 72].

Energy-Consuming Systems

IoT providers that assist with the installation or retrofitting of energy-consuming systems in a business environment will need to assess the energy efficiency of the system using the prescribed permanent measuring instruments and submit a report to the Director-General.[123] If a system does not meet the required energy efficiency, then the provider is responsible for maintenance or other measures to ensure the system meets the standards.[124]

[122] [ref 90] Section 12: Restriction on supply of regulated goods.
[123] [ref 90] Section 26B(2): Minimum energy efficiency standards for energy-consuming systems.
[124] [ref 90] Section 26B(3): Minimum energy efficiency standards for energy-consuming systems; and Section 32: Penalties for non-compliance.

IoT providers should ensure that their products meet the required energy efficiency standards using one of the accredited testing laboratories listed on the NEA's website [ref 73]. Compliance with international standards in this area should assist in meeting the required standards for registration.

Health Products Act

The Health Products Act (HPA) ensures uniform registration and regulation of health products including the manufacture, import, supply, storage, presentation and advertisement of the products [ref 93]. It does not explicitly exclude connected devices or services and therefore it is considered relevant to a variety of health-related IoT products. The two categories of products relevant to IoT providers are "medical device" and "cosmetic product".

The definition of medical device includes software, as well as any instrument, apparatus, implement, machine, appliance, implant, similar related article.[125] This, therefore, can conceivably include IoT products such as medical robots, implants such as glucose monitors or pace makers, temporary and portable medical devices. The definition of "cosmetic products" includes products that come into external contact with the body and may include a variety of devices such as toothbrushes or water picks, laser hair removal devices, UV patch, or hair brushes.[126]

Failure to comply with the HPA registration requirements risks fines between S$10,000 and S$50,000 for individuals (double for corporate bodies) or 2 years imprisonment.[127]

To comply with the HPA, IoT providers should support their product for the lifetime of the product, otherwise they are at risk of[128]:

- Supplying information to the national Authority
- Be required to issue a statement to specific persons or the general public
- Recall the product
- Having use or administration of the product be prohibited
- Any other measure deemed necessary, possibly including fines

Fines or other measures may impact that financial stability of the IoT provider and announcements or recalls may damage its public image.

Registered Health Products

Manufacturers, importers, and wholesalers of health products must be registered. Likewise, only registered products can be supplied in Singapore.[129] In order to obtain registration for a product, the manufacturer, importer or wholesaler may need to have the product

[125] [ref 93] First Schedule, Section 1: Medical device
[126] [ref 93] First Schedule, Section 2: Cosmetic product
[127] [ref 93] Sections 13, 14, 15, and 60.
[128] [ref 93] Section 42(2): Reporting of defects and adverse effects to Authority.
[129] [ref 93] Section 15: Prohibition against supply of unregistered health products.

evaluated, provide samples to the Authority for analysis, and submit a report on any evaluation.[130] When evaluating the health product, the national Authority will determined if a product is of sufficient quality, safe, effective, presented appropriately, complies with any additional requirements or other "relevant" matters.

Singapore's adherence to international standards and best practices can be used a guideline for IoT providers wishing to develop and distribute products for the Singaporean market. Product testing, certification, and compliance with international standards may assist in ensuring and demonstrating that the product is found to be of sound quality, safe, effective, appropriate and complies with any "additional" requirements. As Singapore has not set out a policy on using certification or compliance schemes, IoT providers may consider the options of self-certification or third-third party testing.

Defects in Health Products

If a manufacturer, importer, supplier or registrant of a health product becomes aware of a "defect" in or "adverse effect" from the health product it must be reported to the authority.[131] A product has a defect if[132]:

- It has or has possibly been adulterated or tampered with;
- It is or is possibly a counterfeit or an unwholesome health product;
- It is or is possibly of inadequate quality or unsafe or inefficacious for its intended purpose; or
- It fails or could possibly fail to satisfy such other standards or requirements as may be prescribed.

The definition of a "defect" is quite broad and could encompass a number of IoT-related risks for health devices. For instance, when a new vulnerability is discovered, it may not be possible for the IoT provider to know if or how many heath devices are affected, or "adulterated". It may also be that a health device is found to be a prime target for use in DDoS attacks which may result in the product being deemed of "inadequate quality".
A final example is the transmission of sensitive data in clear text, putting the data at risk of man-in-the-middle attacks, impacting the integrity and confidentiality of the data. In this case, the product may fail to satisfy "other standards or requirements".

IoT products are susceptible to a variety of threats both online and offline. It is important that the devices are supported throughout their lifetime to protect against any "defects" which may impact IoT products' legitimacy in the marketplace. Some techniques for mitigating risk are technical, such as the ability to update software or hardware and protect against known vulnerabilities or the use of encryption for transferring sensitive data. Others are at the organisation-level, such as having a policy and procedure for customer outreach either through the local distributor or direct to user when the consumer needs to be contacted about specific issues or updates for the product.

[130] [ref 93] Section 33(1): Evaluation of health products.
[131] [ref 93] Section 42(1): Reporting of defects and adverse effects to Authority.
[132] [ref 93] Section 42(6): Reporting of defects and adverse effects to Authority.

References

1. Australia. “Competition and Consumer Act 2010, Section 61: Guarantees as to the fitness for particular purpose, etc.” Retrieved from: https://www.legislation.gov.au/Details/C2018C00390
2. Australia. “Competition and Consumer Act 2010, Volume 3, Schedule 2, Section 54: Guarantees as to acceptable quality.” Retrieved from: https://www.legislation.gov.au/Details/C2018C00390
3. Australia. “Competition and Consumer Act 2010, Volume 3, Schedule 2, Section 55: Guarantees as to fitness for any disclosed purpose, etc.”. Retrieved from: https://www.legislation.gov.au/Details/C2018C00390
4. Australia. “Competition and Consumer Act 2010, Volume 3, Schedule 2, Section 143: Making information standards for goods and services.” Retrieved from, https://www.legislation.gov.au/Details/C2018C00390
5. Australia. “Competition and Consumer Act 2010, Volume 3, Schedule 2, Section 58: Guarantees as to repairs and spare parts.” Retrieved from, https://www.legislation.gov.au/Details/C2018C00390
6. Australia. “Competition and Consumer Act 2010”. Retrieved from: https://www.legislation.gov.au/Details/C2018C00390
7. Australia. “Privacy Act 1988, APP 8: Cross-border disclosure of personal information.” Retrieved from: https://www.legislation.gov.au/Details/C2018C00292
8. Australia. “Privacy Act 1988, Section 6D: Small business and small business operators.” Retrieved from: https://www.legislation.gov.au/Details/C2018C00292
9. Australia. “Privacy Act 1988”. Retrieved from: https://www.legislation.gov.au/Details/C2018C00292
10. Australia. “Privacy Amendment (Notifiable Data Breaches) Act 2017, Section 26WL: Entity must notify eligible data breach.” Retrieved from: https://www.legislation.gov.au/Details/C2017A00012
11. Australia. “Privacy Amendment (Notifiable Data Breaches) Act 2017, Section 26WK: Statement about eligible data breach. Retrieved from: https://www.legislation.gov.au/Details/C2017A00012
12. Australia. “Privacy Amendment (Notifiable Data Breaches) Act 2017, Section 26WL: Entity must notify eligible data breach.” Retrieved from: https://www.legislation.gov.au/Details/C2017A00012
13. Australia. “Privacy Amendment (Notifiable Data Breaches) Act 2017”. Retrieved from: https://www.legislation.gov.au/Details/C2017A00012
14. Australian Competition & Consumer Commission. “Legislation: The Competition and Consumer Act 2010.” Retrieved from: https://www.accc.gov.au/about-us/australian-competition-consumer-commission/legislation
15. BBC. “What did she say?! Talking doll Cayla is hacked.” Retrieved from: https://www.bbc.com/news/av/technology-31059893/what-did-she-say-talking-doll-cayla-is-hacked
16. Bird and Bird. “Australian Mandatory Data Breach Notification Guide: Protecting information in an Australian context”. Retrieved from: https://www.twobirds.com/~/media/dataprotectiontoolbrochure_australia_a4_v15digital.pdf?la=en
17. Bundesnetzagentur (Germany). “Bundesnetzagentur removes children’s doll “Cayla” from the market.” Retrieved from: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422
18. Chirgwin, Richard. “ ‘Cyber Kangaroo’ ratings for IoT security? Jump to it, says Austrlia’s cyber security minister”. The Register, October 16, 2017. Retrieved from: https://www.theregister.co.uk/2017/10/16/connected_devices_security_rating_scheme
19. Consumerist. “D-Link Dismissal.” Retrieved from: https://consumerist.com/consumermediallc.files.wordpress.com/2017/09/dlinkdismissal.pdf
20. Consumerist. “These toys don’t just listen to your kid they send what they hear to a defense contractor.” Retrieved from: https://consumerist.com/2016/12/06/these-toys-dont-just-listen-to-your-kid-they-send-what-they-hear-to-a-defense-contractor
21. Consumers International. “Connected Toys”. Retrieved from: https://www.consumersinternational.org/what-we-do/consumer-protection/safer-products/connected-toys
22. Department for Digital, Culture, Media & Sport (UK). “Code of Practice for consumer IoT security.” Retrieved from: https://www.gov.uk/government/publications/secure-by-design/code-of-practice-for-consumer-iot-security
23. Department for Digital, Culture, Media & Sport (UK). “Data Protection Act: General Processing.” Retrieved from: https://www.gov.uk/government/publications/data-protection-act-general-processing

24. Department for Digital, Culture, Media & Sport (UK). "Data Protection Act: Law Enforcement Processing." Retrieved from: https://www.gov.uk/government/publications/data-protection-act-law-enforcement-processing
25. Department for Digital, Culture, Media & Sport (UK). "Data Protection Act: Intelligence Services Processing." Retrieved from: https://www.gov.uk/government/publications/data-protection-act-intelligence-services-processing
26. Department for Digital, Culture, Media & Sport (UK). "Data Protection Act: Information Commissioner and Enforcement." Retrieved from: https://www.gov.uk/government/publications/data-protection-act-information-commissioner-and-enforcement
27. Department of Homeland Security and Department of Justice (USA). "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015." Retrieved from: https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf
28. European Commission. "CE Marking". Retrieved from: https://ec.europa.eu/growth/single-market/ce-marking_en
29. European Commission. "Guidelines on Data Protection Impact Assessment (DPIA)". Retrieved from: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
30. European Commission. "Notified Bodies Nando." Retrieved from: http://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=country.main
31. European Commission. "Single Market for Goods: Notified Bodies." Retrieved from: https://ec.europa.eu/growth/single-market/goods/building-blocks/notified-bodies_en
32. European Commission. "The "Blue Guide" on the implementation of EU products rules 2016." Retrieved from: http://ec.europa.eu/DocsRoom/documents/18027
33. European Commissioner. "CE Marking: Importers and distributors." Retrieved from: https://ec.europa.eu/growth/single-market/ce-marking/importers-distributors_en
34. European Commissioner. "CE Marking: Manufacturers." Retrieved from: https://ec.europa.eu/growth/single-market/ce-marking/manufacturers_en
35. European Council. "Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"). Retrieved from: http://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf
36. European Union Agency for Network and Information Security. "Baseline Security Recommendations for IoT." Retrieved from: https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
37. European Union Article 20 Data Protection Working Party. "Guidelines on Personal data breach notification under Regulation 2016/679". Retrieved at: https://ec.europa.eu/newsroom/document.cfm?doc_id=47741
38. European Union. "General Data Protection Regulation, Article 26: Joint controllers". Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
39. European Union. "General Data Protection Regulation, Article 32: Security of Processing". Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
40. European Union. "General Data Protection Regulation, Article 4: Definitions". Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
41. European Union. "General Data Protection Regulation, Article 83: General conditions for imposing administrative fines." Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
42. European Union. "General Data Protection Regulation". Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
43. European Union. "Network and Information Security Directive, Article 16(4): Security of the network and information systems of digital service providers". Retrieved from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
44. European Union. "Network and Information Security Directive, Article 15: Implementation and enforcement." Retrieved from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
45. European Union. "Network and Information Security Directive". Retrieved from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

46. Federal Trade Commission. “ASUS Settles FTC Charges That Insecure Home Routers and “cloud” services Put Consumers’ Privacy at Risk”. Retrieved from: https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put
47. Federal Trade Commission. “Children’s Online Privacy Protection Rule (“COPPA”), Section 312.3: Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.” Retrieved from: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
48. Federal Trade Commission. “Children’s Online Privacy Protection Rule (“COPPA”), Section 312.2: Definitions”. Retrieved from: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
49. Federal Trade Commission. “Children’s Online Privacy Protection Rule (“COPPA”), Section 312.5(2): Parental consent”. Retrieved from: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
50. Federal Trade Commission. “Children’s Online Privacy Protection Rule (“COPPA”)”. Retrieved from: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
51. Federal Trade Commission. “Complaint for Permanent Injunction and Other Equitable Relief.” Retrieved from: https://www.ftc.gov/system/files/documents/cases/170105_d-link_complaint_and_exhibits.pdf
52. Federal Trade Commission. “Federal Trade Commission Act, Section 45(a(4(A-B))): Unfair methods of competition unlawful; prevention by Commission.” Retrieved from: https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act
53. Federal Trade Commission. “Federal Trade Commission Act”. Retrieved from: https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act
54. Federal Trade Commission. “FTC Charges D-Link Put Consumers’ Privacy at Risk Due to the Inadequate Security of its Computer Routers and Cameras.” Retrieved from: https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate
55. Federal Trade Commission. “FTC Publishes Inflation-Adjusted Civil Penalty Amounts”. Retrieved from: https://www.ftc.gov/news-events/press-releases/2018/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts
56. Federal Trade Commission. “FTC Warns Operator Group, Tinitel that Online Services Might Violate COPPA”. Retrieved from: https://www.ftc.gov/news-events/press-releases/2018/04/ftc-warns-gator-group-tinitell-online-services-might-violate
57. National Institute of Standards and Technology (NIST, USA). “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks.” Retrieved from: https://csrc.nist.gov/publications/detail/nistir/8228/draft
58. Gemalto. “90% of Consumers Lack Confidence in the Security of IoT Devices, Finds Gemalto Study”. Retrieved from: https://blog.gemalto.com/security/2017/10/31/90-consumers-lack-confidence-security-iot-devices-finds-gemalto-study
59. Greenberg, Andy. “Hackers Remotely Kill a Jeep on the Highway – With Me in It.” Wired, July 21, 2015. Retrieved from: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway
60. Hern, Alex. “Revolv devices bricked as Google’s Next shuts down smart home company.” The Guardian, April 5, 2016. Retrieved from: https://www.theguardian.com/technology/2016/apr/05/revolv-devices-bricked-google-nest-smart-home
61. Industry Expert 1. *Expert interview,* September 2018.
62. Industry Expert 2. *Expert Interview*, September 2018.
63. Information Commissioner’s Office (UK). “Data sharing code of practice.” Retrieved from: https://ico.org.uk/media/for-organizations/documents/1068/data_sharing_code_of_practice.pdf
64. Information Commissioner’s Office (UK). “Direct Marketing Code”. Retrieved from: https://ico.org.uk/media/1555/direct-marketing-guidance.pdf
65. Information Commissioner’s Office (UK). “Guide to Law Enforcement Processing (Part 3 of the DP Act 2018)”. Retrieved from: https://ico.org.uk/for-organizations/guide-to-law-enforcement-processing-part-3-of-the-dp-act-2018
66. Information Commissioner’s Office (UK). “The Principles”. Retrieved from: https://ico.org.uk/for-organizations/guide-to-the-general-data-protection-regulation-gdpr/principles
67. IoT Security Foundation. “IoT Security Compliance Framework”. Retrieved from: https://www.iotsecurityfoundation.org/best-practice-guidelines

68. IoT Security Foundation. “UK Government moves towards regulating security in consumer IoT”. Retrieved from: https://www.iotsecurityfoundation.org/uk-government-moves-towards-regulating-security-in-consumer-iot
69. Kirk, Jeremy. “Backdoor found in D-Link router firmware code.” InfoWorld, October 14, 2013. Retrieved from: https://www.infoworld.com/article/2612384/network-router/backdoor-found-in-d-link-router-firmware-code.html
70. Lexology. “California Enacts First IOT Security Law in U.S.”. Retrieved from: https://www.lexology.com/library/detail.aspx?g=7009330f-592b-4318-bb11-a0eca0148be9
71. National Environment Agency (Singapore). “About Mandatory Energy Labelling and Minimum Energy Performance Standards.” Retrieved from: https://www.nea.gov.sg/our-services/climate-change-energy-efficiency/energy-efficiency/household-sector/about-mandatory-energy-labelling-and-minimum-energy-performance-standards
72. National Environment Agency (Singapore). “Regulated Goods”. Retrieved from: https://www.nea.gov.sg/our-services/climate-change-energy-efficiency/energy-efficiency/household-sector/regulated-goods
73. National Environment Agency (Singapore). “Test Laboratories.” Retrieved from: https://www.nea.gov.sg/our-services/climate-change-energy-efficiency/energy-efficiency/household-sector/test-laboratories
74. National Institute of Standards and Technology (USA). “Cybersecurity Framework”. Retrieved from: https://www.nist.gov/cyberframework
75. National Institute of Standards and Technology (USA). “Privacy Engineering Program”. Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering
76. Now updated to the 2010 version in English law. United Kingdom. “Third Parties (Rights against Insurers) Act 2010). Retrieved from: https://www.legislation.gov.uk/ukpga/2010/10/contents
77. Office of the Australian Information Commissioner. “Guide to Data Analytics and the Australian Privacy Principles.” Retrieved from: https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-data-analytics-and-the-australian-privacy-principles
78. Office of the Australian Information Commissioner. “Privacy fact sheet 17”. Retrieved from: https://www.oaic.gov.au/resources/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles.pdf
79. Pen Test Partners. “Totally Pwning the Tapplock Smart Lock.” Retrieved from: https://www.pentestpartners.com/security-blog/totally-pwning-the-tapplock-smart-lock
80. Ross, Andrew. “IoT adoption perceived as risky, as failures plague 64% of users worldwide”. Information Age, August 21, 2018. Retrieved from: https://www.information-age.com/iot-adoption-123474305
81. See UK National Cyber Security Centre. “Introduction to the NIS Directive”. Retrieved from: https://www.ncsc.gov.uk/guidance/introduction-nis-directive
82. Singapore Standards eShop. “Guidelines for IoT security for smart nation.” Retrieved from: https://www.singaporestandardseshop.sg/product/product.aspx?id=3ee3386a-4332-45be-903b-afef1dfb6770
83. Singapore. “Application of English Law Act, Second Schedule, Section 4: The Insurance Act.” Retrieved from: https://sso.agc.gov.sg/Act/AELA1993
84. Singapore. “Application of English Law Act, Second Schedule, Section 4: The Supply of Goods and Services Act 1982.” Retrieved from: https://sso.agc.gov.sg/Act/AELA1993
85. Singapore. “Application of English Law Act, Second Schedule, First Schedule, Section 3: Unfair Contract Terms Act 1977.” Retrieved from: https://sso.agc.gov.sg/Act/AELA1993
86. Singapore. “Application of English Law Act”. Retrieved from: https://sso.agc.gov.sg/Act/AELA1993
87. Singapore. “Energy Conservation Act, Section 12: Restriction on supply of regulated goods.” Retrieved from: https://sso.agc.gov.sg/Act/ECA2012
88. Singapore. “Energy Conservation Act, Section 26B(3): Minimum energy efficiency standards for energy-consuming systems.” Retrieved from: https://sso.agc.gov.sg/Act/ECA2012
89. Singapore. “Energy Conservation Act, Section 32: Penalties for non-compliance.” Retrieved from: https://sso.agc.gov.sg/Act/ECA2012
90. Singapore. “Energy Conservation Act”. Retrieved from: https://sso.agc.gov.sg/Act/ECA2012
91. Singapore. “Health Products Act, Section 42(6): Reporting of defects and adverse effects to Authority.” Retrieved from: https://sso.agc.gov.sg/Act/HPA2007
92. Singapore. “Health Products Act, Sections 13, 14, 15, and 60”. Retrieved from: https://sso.agc.gov.sg/Act/HPA2007

93. Singapore. “Health Products Act”. Retrieved from: https://sso.agc.gov.sg/Act/HPA2007
94. Tan, Aaron. “Singapore government outlines its approach to IoT”. Computer Weekly, March 21, 2018. Retrieved from: https://www.computerweekly.com/news/252437239/Singapore-government-outlines-its-approach-to-IoT
95. The European Consumer Organisation (BEUC). “Consumer organisations across the EU take action against flawed internet-connected toys.” Retrieved from: https://www.beuc.eu/publications/consumer-organisations-across-eu-take-action-against-flawed-internet-connected-toys/html
96. United Kingdom. “Consumer Rights Act, Section 19(3,9,11), Consumer’s rights to enforce terms about goods”. Retrieved at: http://www.legislation.gov.uk/ukpga/2015/15/contents
97. United Kingdom. “Consumer Rights Act, Section 2(9): Key definitions.” Retrieved from: http://www.legislation.gov.uk/ukpga/2015/15/contents
98. United Kingdom. “Consumer Rights Act, Section 34, Digital content to be of satisfactory quality.” Retrieved from: http://www.legislation.gov.uk/ukpga/2015/15/contents
99. United Kingdom. “Consumer Rights Act, Section 42, Consumer’s rights to enforce terms about digital content.”: Retrieved from: http://www.legislation.gov.uk/ukpga/2015/15/contents
100. United Kingdom. “Consumer Rights Act, Section 46(1), Remedy for damage to device or to other digital content.” Retrieved from: http://www.legislation.gov.uk/ukpga/2015/15/contents
101. United Kingdom. “Consumer Rights Act”. Retrieved from: http://www.legislation.gov.uk/ukpga/2015/15/contents
102. United Kingdom. “Corporate Bodies’ Contracts Act 1960”. Retrieved from: https://www.legislation.gov.uk/ukpga/Eliz2/8-9/46/contents
103. United Kingdom. “Digital Economy Act, Part 5, Chapter 1: Public service delivery.” Retrieved from: http://www.legislation.gov.uk/ukpga/2018/12/contents
104. United Kingdom. “Data Protection Act 2018, Section 14: Automated decision-making authorised by law: safeguards”. Retrieved from: http://www.legislation.gov.uk/ukpga/2018/12/contents
105. United Kingdom. “Data Protection Act 2018, Section 9: Child’s consent in relation to information society services”. Retrieved from: http://www.legislation.gov.uk/ukpga/2018/12/contents
106. United Kingdom. “Digital Economy Act, Section 96: Direct marketing.” Retrieved from: http://www.legislation.gov.uk/ukpga/2018/12/contents
107. United Kingdom. “Data Protection Act 2018”. Retrieved from: http://www.legislation.gov.uk/ukpga/2018/12/contents
108. United Kingdom. “Digital Economy Act, Part 1: Access to digital services; and Part 2: Digital Infrastructure.” Retrieved from: http://www.legislation.gov.uk/ukpga/2017/30/contents
109. United Kingdom. “Digital Economy Act”. Retrieved from: http://www.legislation.gov.uk/ukpga/2017/30/contents
110. United Kingdom. “Guidance: Secure by Design”. Retrieved from: https://www.gov.uk/government/publications/secure-by-design
111. United Kingdom. “Insurance Act 2015.” Retrieved from: http://www.legislation.gov.uk/ukpga/2015/4/contents/enacted
112. United Kingdom. “Misrepresentation Act 1967”. Retrieved from: https://www.legislation.gov.uk/ukpga/1967/7/contents
113. United Kingdom. “Partnership Act 1890”. Retrieved from: http://www.legislation.gov.uk/ukpga/Vict/53-54/39/contents
114. United Kingdom. “Sale of Goods Act 1979”. Retrieved from: https://www.legislation.gov.uk/ukpga/1979/54/contents
115. United Kingdom. “Supply of Goods and Services Act 1892.” Retrieved from: https://www.legislation.gov.uk/ukpga/1982/29/contents
116. United Kingdom. “Unfair Contract Terms Act 1977.” Retrieved from: https://www.legislation.gov.uk/ukpga/1977/50/contents
117. United States Congress. “S.1691 – Internet of Things (IoT) Cybersecurity Improvement Act of 2017”. Retrieved from: https://www.congress.gov/bill/115th-congress/senate-bill/1691/text
118. United States of America. “Cybersecurity Information Sharing Act, Section 5(d): Information shared with or provided to the federal government.” Retrieved from: https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability

119. United States of America. “Cybersecurity Information Sharing Act”. Retrieved from: https://www.federalregister.gov/documents/2016/06/15/2016-13742/cybersecurity-information-sharing-act-of-2015-final-guidance-documents-notice-of-availability
120. Hill, Kashmir and Surya Mattu. “The House That Spied on Me” Williams, Kevin. Gizmodo, July 2, 2018. Retrieved from: https://gizmodo.com/the-house-that-spied-on-me-1822429852
121. Yonhap News Angency. “Regulations on IoT industry will be eased: ministry.” Retrieved from: http://english.yonhapnews.co.kr/business/2016/05/18/0504000000AEN20160518006700320.html
122. Government Publishing Office (USA). “U.S. Safe Web Act of 2006”. Retrieved from: https://www.gpo.gov/fdsys/pkg/PLAW-109publ455/content-detail.html
123. Department for Business, Energy and Industrial Strategy (UK). “Consumer Rights Act 2015”. Retrieved from: https://www.gov.uk/government/publications/consumer-rights-act-2015/consumer-rights-act-2015
124. Federal Trade Commission (USA). “Complying with COPPA: Frequently Asked Questions”. Retrieved from: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

www.iotsecurityfoundation.org