IoT Cybersecurity: Regulation Ready

A Landscape Report – Concise Version

Contents

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. 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[1] 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 41], (dis)trust [ref 28], and security concerns [ref 20]. 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 [ref 42]. 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 [ref 23].

[1] 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 fibre 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.[2] 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.

[2] 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[3]
General Data Protection Regulation (EU) [ref 13]	€10 million up to 2% global turnover or, €20 million up to 4% global turnover
Federal Trade Commission Act (USA) [ref 17]	$41,484 (per violation, per day)
Digital Economy Act (UK) [ref37]	£20,000 a day not to exceed 10% of gross revenue
Privacy Act 1988 and Notifiable Data Breaches Acts (Australia) [ref 4]	A$420,000 (individuals) A$2.1 million (corporations)
Health Products Act (Singapore) [ref 33]	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[4] is 13, while GDPR sets the age at 16 [ref 36]. 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 3]. 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 12].

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 [ref 5]. 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 21].

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

[3] 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.

[4] 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.

Actions such as information gathering/logging, data mapping, and internal policies and procedures may support compliance activities, such as cybersecurity certifications or conformity assessments.[5] 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' for 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 7], the USA's NIST Cybersecurity Framework [ref 25] and Privacy Engineering Program [ref 26] or using internationally recognised frameworks such as the IoT Security Foundation's (IoTSF) Security Compliance Framework [ref 22].

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

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 of the full report.

European Union

Overview

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

CE Marking ensures the safety, health, and environmental protections of products on the market in the EU [ref 9]. Applicable product categories and regulations may be updated at any time, underlining regulation's shifting landscape. CE marking and associated 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 [ref 13]. 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.

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'.

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) [ref 41]. 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.

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)

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 16]. 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 to children's smart watches [refs 18, 42]. In practice, the fines can quickly mount up.[6] 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.

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

[6] 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 [ref 39]. 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. 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 8].

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 15]. 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, including third parties such as cloud providers and web services.

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 (including third parties such as cloud providers and web services)	• Data protection policy • 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)

The **Data Protection Act 2018 (DPA)** is the UK's primary data protection legislation and implements GDPR at the local level [ref 36]. 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. 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 [ref 35]. Digital content is broadly defined as "data which are produced and supplied in digital form" and must be of "satisfactory quality".

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. 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 37].

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. IoT providers in the gas and electric, and water and sewerage sectors will be subject to information sharing and processing requirements, and IoT devices which may be at risk of or are intended to receive marketing materials and spam may be subject to additional requirements.

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)

The **Privacy Act** sets out 13 Australian Privacy Principles (APPs) applicable to local and extraterritorial companies processing personal information [ref 2]. 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. 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 3].

In addition, the company is automatically required to notify affected individuals or provide a public statement on the event for *all* notifiable data breaches. 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 13].

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 1]. Products must be fit for purpose, free from defects and safe. 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. 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.

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)

.

The original **Application of English Law Act (AELA)** was enacted in 1993 [ref 31]. Its purpose is to clarify the "extent to which English law is applicable in Singapore", as well as any updates to existing laws. 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, Supply of Goods and Services Act, and Unfair Contract Terms Act, all have amendments included in the AELA text.

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 92]. 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. 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 33]. 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. 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 40]. 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 38, 10]. However, others have only hinted at ideas for future regulation. For instance, Australia is reportedly assessing a consumer rating system for IoT products [ref 6].

Jurisdiction	Regulation or Policy	Status
European Union (EU)	EU Cybersecurity Act (Regulation) [ref 10]	Trialogue final text negotiations
USA	Internet of Things (IoT) Cybersecurity Improvement Act [ref 38]	Introduced in the Senate
California (USA)	Security of Connected Devices Act [ref 24]	Effective 1 January 2020
UK	Code of Practice for Consumer IoT Security [ref 7]	The UK has signposted the Code of Practice as a base of future regulatory action [ref 23]. 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 34]	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 11]
- USA's NIST Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (draft guidance) [ref 19]
- UK's Code of Practice for Consumer IoT [ref 7]
- Australia's Guide to Data Analytics and the Australian Privacy Principles [ref 27]
- Singapore's Guidelines for IoT security for smart nation [ref 29]

References

1. Australia. “Competition and Consumer Act 2010”. Retrieved from: https://www.legislation.gov.au/Details/C2018C00390
2. Australia. “Privacy Act 1988”. Retrieved from: https://www.legislation.gov.au/Details/C2018C00292
3. Australia. “Privacy Amendment (Notifiable Data Breaches) Act 2017”. Retrieved from: https://www.legislation.gov.au/Details/C2017A00012
4. 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
5. 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
6. 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
7. 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
8. 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
9. European Commission. “CE Marking”. Retrieved from: https://ec.europa.eu/growth/single-market/ce-marking_en
10. 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
11. 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
12. European Union Article 20 Data Protection Working Party. “Guidelines on Personal data breach notification under Regulation 2016/679”. Retrieved from: https://ec.europa.eu/newsroom/document.cfm?doc_id=47741
13. European Union. “General Data Protection Regulation”. Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679
14. European Union. “Network and Information Security Directive”. Retrieved from: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
15. 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
16. Federal Trade Commission. “Federal Trade Commission Act”. Retrieved from: https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act
17. Federal Trade Commission. “FTC Publishes Inflation-Adjusted Civil Penalty Amounts”. Retrieved at: https://www.ftc.gov/news-events/press-releases/2018/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts
18. Federal Trade Commission. “FTC Warns Operator Group, Tinitel that Online Services Might Violate COPPA.” https://www.ftc.gov/news-events/press-releases/2018/04/ftc-warns-gator-group-tinitell-online-services-might-violate
19. 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

20. 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
21. Industry Expert 2. *Expert Interview*, September 2018.
22. IoT Security Foundation. “IoT Security Compliance Framework”. Retrieved from: https://www.iotsecurityfoundation.org/best-practice-guidelines
23. 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
24. 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
25. National Institute of Standards and Technology (USA). “Cybersecurity Framework”. Retrieved from: https://www.nist.gov/cyberframework
26. National Institute of Standards and Technology (USA). “Privacy Engineering Program”. Retrieved from: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering
27. 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
28. 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
29. 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
30. Singapore. “Application of English Law Act, Second Schedule, Section 4: The Insurance Act.” Retrieved from: https://sso.agc.gov.sg/Act/AELA1993
31. Singapore. “Application of English Law Act”. Retrieved from: https://sso.agc.gov.sg/Act/AELA1993
32. Singapore. “Energy Conservation Act”. Retrieved from: https://sso.agc.gov.sg/Act/ECA2012
33. Singapore. “Health Products Act”. Retrieved from: https://sso.agc.gov.sg/Act/HPA2007
34. 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
35. United Kingdom. “Consumer Rights Act”. Retrieved from: http://www.legislation.gov.uk/ukpga/2015/15/contents
36. United Kingdom. “Data Protection Act 2018”. Retrieved from: http://www.legislation.gov.uk/ukpga/2018/12/contents
37. United Kingdom. “Digital Economy Act”. Retrieved from: http://www.legislation.gov.uk/ukpga/2017/30/contents
38. 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
39. 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
40. Yonhap News Angency. “Regulations on IoT industry will be eased: ministry.” Retrieved from: http://english.yonhapnews.co.kr/business/2016/05/18/0504000000AEN20160518006700320.html
41. 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
42. 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

www.iotsecurityfoundation.org