CyBOK

LAW AND REGULATION

KNOWLEDGE AREA

(DRAFT FOR COMMENT)

AUTHOR: Robert Carolina

Royal Holloway, University of London

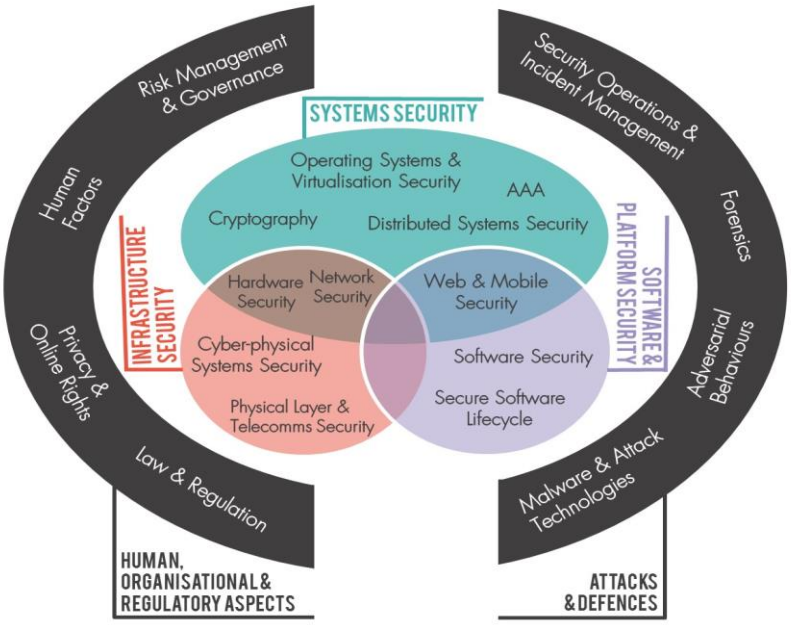
EDITOR: Howard Chivers – University of York

REVIEWERS:

Tom Holt – Michigan State University

* Further reviews pending

Following wide community consultation with both academia and industry, 19 Knowledge Areas (KAs) have been identified to form the scope of the CyBOK (see diagram below). The Scope document provides an overview of these top-level KAs and the sub-topics that should be covered under each and can be found on the project website: https://www.cybok.org/.



We are seeking comments within the scope of the individual KA; readers should note that important related subjects such as risk or human factors have their own knowledge areas.

It should be noted that a fully-collated CyBOK document which includes issue 1.0 of all 19 Knowledge Areas is anticipated to be released by the end of July 2019. This will likely include updated page layout and formatting of the individual Knowledge Areas.

Law and Regulation

Robert Carolina

July 2019

INTRODUCTION

The purpose of this knowledge area is to provide a snapshot of legal and regulatory topics that merit consideration when conducting various activities in the field of cyber security such as: security management, risk assessment, security testing, forensic investigation, research, product and service development, and cyber operations (defensive and offensive). The hope is to provide a framework that shows the cyber security practitioner the most common categories of legal and regulatory risk that apply to these activities, and to highlight (where possible) some sources of legal authority and scholarship on these topics.

The nature and breadth of the subject matter addressed renders this knowledge area, and the sources cited, a mere starting rather than ending point. Undoubtedly, some favoured, even significant, sources of authority and scholarship have been overlooked.

The reader is assumed to hold no formal qualification or training in the subject of law. The audience is further assumed to be multinational. To make the material practically accessible to such a diverse body of cyber security domain specialists, subjects are presented at a level that would be considered introductory for those who are already well educated in law or public policy.

The rules of mathematics and physical sciences are both immutable and identical around the world. Laws and regulations are not. The foundation of the world's legal and regulatory systems has for many centuries been based on the principle of territorial sovereignty. Various international efforts to harmonise differences in laws and regulations have met with variable degrees of success. In practice, this means that laws and regulations differ – sometimes significantly – from state to state. These differences are not erased simply because people act through the instrumentality of cyberspace [1].

This knowledge area, however, addresses a multinational audience of practitioners who will be called upon to conduct their activities under laws and regulations imposed by different states - both the home state in which they practice, and foreign states with which they make contact. While respecting the reality that legal details vary by state, this knowledge area will attempt to identify some widely shared norms among various systems of domestic law and regulation, and some aspects of public international law, that may (or should) influence the work of the security practitioner.

In the search for generalisable norms that retain utility for the practitioner, this knowledge area focuses primarily on substantive law. Substantive law focuses on the obligations, responsibilities, and behaviours, of persons. Examples include computer crime, contract, tort, data protection, etc.

Procedural rules are mostly excluded from coverage. Procedural rules tend to focus on managing the dispute resolution process or specifying methods of communication with a state authority. Examples include civil procedure,[1] criminal procedure,[2] and rules of evidence.[3] Although these are significant to the administration of justice, they are often parochial in nature and bound up with quirks of local practice. Cyber security practitioners who need to become familiar with the details of these rules (e.g., forensic investigators, law enforcement officers, expert witnesses, and others who collect or present evidence to tribunals) invariably require specialist guidance or training from relevant local legal practitioners who understand the procedural rules of a given tribunal.[4]

As with many efforts at legal taxonomy, the difference between substance and procedure is imprecise at the boundary. The test for inclusion in this knowledge area is less to do with divining the boundary between substance and procedure, and springs instead from the desire to make normative statements that remain useful to practitioners in a multinational context.

Section 1 starts the knowledge area with an introduction to principles of law and legal research, contrasting the study of law and science and explaining the role of evidence and proof. Section 2 then explores various aspects of jurisdiction in an online environment.

Sections 3 and 4 discuss general principles of privacy law (including interception of communications) and the more detailed regulatory regime of data protection law. Section 5 presents an outline of computer crime laws, and more specifically crimes against information systems.

Sections 6 and 7 provide an introduction to principles of contract and tort law of interest to practitioners. Section 8 provides a general introduction to relevant topics in intellectual property, while Section 9 provides an overview of laws that reduce liability of content intermediaries.

Sections 10 and 11 address a few specialist topics, with an exploration of rights and responsibilities in trust services systems and a brief survey of other topics of interest such as export restrictions on cryptography products. Sections 12, 13, and 14, conclude the knowledge area with a survey of public international law, ethics, and a checklist for legal risk management.

Finally, the author of this knowledge area is trained in the common law[5] (nearly ubiquitous in anglophone territories) and experienced in international commercial legal practice conducted in London. Examples of legal norms are drawn from common law (as interpreted by different states), various anglophone statutes, European Union law, and public international law.[6] The author welcomes thoughtful correspondence confirming, further qualifying, or challenging the normative status of issues presented.

CONTENT

1 Introductory principles of law and legal research

Cyber security practitioners and researchers come from an incredibly wide array of educational backgrounds. Experience teaching legal and regulatory subjects to cyber security post-graduate students, and providing legal advice to cyber security practitioners, suggests that much of this knowledge area's content will be novel to those whose education is based in science, technology, engineering, mathematics, many social sciences, and many of the humanities. These introductory observations are offered as an aid for those who are approaching the subject without significant experience.

1.1 The nature of law and legal analysis

Although the reader is assumed to have some degree of familiarity with the process of law making and law enforcement, a review of some of the most common sources of law should help to orient those who are unfamiliar with legal research and analysis.

Law should be analysed with rigorous logic. Unlike scientific disciplines such as physics or mathematics, however, the study of law is not conceptualised as an effort to discover immutable principles of our world. Law is bound together with social and political values, human desire, and human frailty [2].

Although law might be conceptualised by some as a sort of logical clockwork system of intricate moving parts, society influences the development and interpretation of law even as law influences the behaviour of members of society. Societies evolve and values change. Changes to law and to methods of interpreting law tend to follow.[7] This creates a number of challenges for legal scholarship,[8] as the topic under study is itself undergoing a process of change.[9] Perhaps as a result the study

of law is often presented in the form of historical dialectic: examining the evolution of law and its interpretation over time, often through case studies. This method of presenting information both aids in the interpretation of law as it exists and suggests the direction of future developments.

The study of law endeavours to share at least one characteristic with the sciences: the ability to predict outcomes. While sciences like chemistry predict the outcome of events such as the introduction of solid sodium to liquid water, the study of law attempts to predict the outcome of disputes when introduced to a suitably expert legal tribunal. Although the study of law can never predict outcomes of dispute with 100% certainty, in states with well-developed systems of law and well-qualified adjudicators, it is possible to achieve a degree of predictability of outcome that is sufficiently high to maintain confidence in the system as a whole.[10]

Legal studies often begin with a mechanistic review of the governance processes surrounding the adoption and enforcement of law. Laws are made (legislative authority), laws are interpreted (judicial authority), and laws are enforced (executive authority). Understanding different governance structures adopted by states to manage these three processes requires an examination of comparative constitutional law which is beyond the scope of this knowledge area.

Most legal research and analysis proceeds on the basis of argument from authority, drawn from an analysis of historical texts that embody expressions of law. There follow a few observations about differing sources of legal authority and how these vary in different contexts. No standards body exists to harmonise the definition of legal terms of art as they are used by different states. Confusion over legal terminology is therefore commonplace in a multinational context.

Primary legislation. In both common law[11] and civil law[12] jurisdictions, primary legislation (typically a statute such as an Act of Congress in the US, or an Act of Parliament in the UK) is the most easily understood embodiment of 'the law'. In civil law jurisdictions primary legislation typically takes the form of adopting or amending a comprehensive legal code.[13] A statute (a law promulgated by a legislature) should be distinguished from a bill (a draft law which may or may not be adopted as a statute)[14] which normally has no force of law.[15]

Secondary legislation. Sometime a degree of law-making authority is delegated by a senior legislative body (such as the UK Parliament or the US Congress) to some other agency of the state (such as the US Commerce Department or the Foreign Minister of the UK). Delegation is often made for reasons of technical expertise, or the need for frequent periodic review of adopted rules. Laws promulgated by such subordinate agencies are generally termed secondary legislation. The term 'regulation' is sometimes used colloquially to refer to secondary legislation as distinct from primary legislation.

European Union legislation. A 'Directive' of the European Union (formerly European Economic Community) is a specific type of primary legislation addressed to the member states of the Union. Each member state is required to examine the terms of the Directive, and then to implement these terms within its own domestic law within a specified time frame. Directives are normally said to lack 'direct effect' in member state law, with some exceptions. By contrast, a European Union 'Regulation' constitutes immediately applicable binding law within all member states.[16]

Judicial decisions. In common law jurisdictions, the published decisions of domestic courts that interpret the law tend to constitute significant and binding interpretative authority depending upon the seniority and jurisdiction of the court. Decisions by the courts of foreign states may constitute persuasive authority, or indeed their interpretation of the law may be ignored entirely.[17] In civil law jurisdictions, the decisions of judges are generally accorded less authority than similar decisions in a common law jurisdiction.

Codes. In legal research, 'code' can refer to any systemised collection of primary legislation,[18] secondary legislation,[19] model laws,[20] or merely a set of rules published by public or private organisations.[21]

Restatements of the law. A restatement of the law is a carefully constructed work, normally un-

dertaken by a committee of legal experts over a number of years, which seeks to explain, clarify, and codify existing law. Although restatements are not normally considered a source of mandatory authority, as carefully considered expressions of expert opinion they are often extremely influential.[22]

Treaties. Treaties are instruments of agreement among and between states. In some states, the legal terms of a treaty are automatically carried into operation of a contracting state's domestic law once the state has fully acceded to the treaty. In others, domestic law is not amended unless and until the domestic legislature acts to amend domestic law in accordance with the treaty requirements. (Public international law is discussed in section 12.)

Scholarly articles. Within common law jurisdictions, scholarly articles written by legal academics can constitute a type of persuasive, albeit weak, authority. Judges typically adopt the arguments of legal scholars only to the extent that the scholar's work persuades a jurist to adopt their view. In many civil law systems, by contrast, scholarly articles by leading legal academics may be accorded significant deference by tribunals who are called upon to interpret the law.

1.2 Applying law to cyberspace

The birth of cyberspace caused a great deal of anxiety with regard to the application of laws and regulations to this new domain.

Two prevailing schools of thought emerged. The first school posited that cyberspace is so radically different from anything in human experience, that old laws were unsuitable and should be widely inapplicable to actions taken using this new domain. Law makers and judges were encouraged by this school to re-examine all doctrines afresh and to abandon large swathes of precedent when considering disputes. Radical proponents of this view went so far as to deny the authority of sovereign states to enforce laws and regulations in the context of Internet-related activities [3].

The second school held instead that the Internet is, like so many tools developed in human history, merely an instrumentality of human action. As such, laws could – and perhaps should – continue to be applied to persons who use cyberspace in most respects just as they applied before it existed [4, 5, 6]. Members of this second school described a 'cyberspace fallacy' – the false belief that cyberspace was a legal jurisdiction somehow separate and distinct from real space [7].

For the time being, the second school has almost universally prevailed with state authorities [1, 8, 9]. The practitioner is confronted with the reality that existing laws, some centuries old and some amended or born anew each year, are applied by states, their law makers, judges, police and defence forces to cyberspace-related activity whether or not cyberspace was expressly contemplated by those same laws.[23]

One must be cautious when attempting to map legal rules onto activities. While lawyers and legal scholars make every effort to divide the law into neat categories, real-life and cyber operations do not always fit neatly into a single taxonomic category. For example, a single data processing action that does not infringe copyright and is not defamatory may still constitute a violation of data protection rights. Any given action should be assessed by reference to whatever laws or regulations might present risk. The problem of conflicting obligations that can arise as a result of multi-state regulation is introduced in Section 2.

1.3 The nature of evidence and proof

The concept of 'proof' in law is different from the term as it is used in the field of mathematics or logic. This can create confusion in discussions of cyber security topics and the law. Clarifying the difference also aids in understanding the role of evidence in law.

As a gross generalisation, legal analysis in the context of a dispute proceeds in two steps. First, a 'fact finder' (a judge, jury, regulator, etc.) has to consider competing versions of events and to establish a

factual narrative or 'finding'. Once this factual narrative is established, it is then subjected to analysis under applicable law and regulation.

In law to 'prove' something means simply to use permissible evidence in an effort to demonstrate the truth of contested events to a fact finder to a prescribed degree of certainty. In this context, 'permissible evidence' can take a variety of forms. Subject to the rules and limitations of different legal systems, this can include direct witness testimony, business records, correspondence, surveillance records, data logs, etc.[24]

The applicable standard of proof, which is to say the degree of certainty that must be achieved by the fact finder to issue a given finding, in turn depends upon the issue under consideration. A non-exhaustive sample of different standards of proof used in various legal contexts is presented in Table 1.

1.4 Distinguishing criminal and civil law

Criminal law is the body of law that prohibits behaviour generally abhorred by society. Criminal law is normally enforced by an agency of the state. Examples include prohibitions against bank fraud and computer hacking. Depending upon the society in question, the purposes of criminal law are usually described as some combination of:

- deterrence (seeking to deter bad behaviour, for both members of society generally and a criminal specifically);
- incapacitation (limiting the ability of the criminal to further harm society);
- retribution (causing a criminal to suffer some type of loss in response to crime);
- restitution (causing a criminal to compensate a victim or some related person);
- rehabilitation (seeking to change the long-term behaviour of a criminal).

Terms such as 'guilty' and 'innocent' are normally reserved as descriptions of verdicts (outcomes) in a criminal case. These terms should not be used when referring to outcomes of civil actions.

Punishments available in criminal law include custodial prison sentences, criminal fines normally remitted to the state, seizure and forfeiture of criminal proceeds, and financial or other restitution remitted to victims.

Most criminal laws require proof of criminal intent by the accused *mens rea*. This is normally a requirement for the state to prove that the accused intended to perform the actions which are defined as criminal. There is normally no requirement for an accused to have understood that their actions were defined as criminal, although some crimes are defined in a fashion that guilt only attaches if it proven that the accused was aware that they were doing something 'wrong'.[26] An accused, therefore, may not be able to escape criminal liability by suggesting, or even proving, that an act was undertaken with good intentions or otherwise 'in the public interest'.[27]

Civil law[28] is the area of law that regulates private relationships among and between persons. Examples include the laws of contract and negligence. A person injured as a result of breach of civil law can normally bring legal action against the responsible party.

Remedies available under civil law (depending on the circumstances) may include some combination of:

- an order for the liable party to pay compensation to the injured party;
- an order to terminate some legal relationship between the parties;

Standard of proof	Degree of Certainty Required	Example context
Beyond a reasonable doubt.	Extremely high. Almost incontrovertible. No other reasonable explanation exists to make sense of the evidence.	This, or a similar standard, is most commonly required for a fact finder to hold an accused person guilty of a crime. This standard is heavily influenced by notions of human rights law because individual life and liberty are at stake.
Clear and convincing evidence.	Reasonably high certainty. Much more than simply 'probable'.	This standard of proof is used in US law, for example, when a court is asked to invalidate a previously granted patent. The burden of proof is set high because this constitutes a deprivation of the property rights previously granted by the US patent office. This phrase is also used to describe the standard adopted by US federal courts when reviewing post-conviction *habeas corpus* petitions to invalidate a criminal conviction long after the normal routes of appeal have been exhausted. In this circumstance, the higher standard is required as a means of preserving the integrity of the original criminal justice process while not foreclosing all possibility of post-conviction review.[25]
Preponderance of evidence. Balance of probabilities.	More probable than not. Greater than 50%. When weighed on the scales of justice, the evidence on one side is at least a feather-weight greater than the other.	The most common standard of proof required to prevail in a civil case.
Probable cause.	The evidence suggests that the target of an investigation has committed a crime, although evidence is not yet conclusive.	The standard required in the US to persuade a judicial officer to issue a search warrant or arrest warrant. This standard serves to filter out trivial or unsubstantiated requests to intrude into privacy or detain a suspect.
Reasonable suspicion.		The standard typically required in the US to justify a police officer temporarily stopping and questioning a person. This lower standard is often justified on policy grounds of minimising threats to the safety of police officers. This phrase has also been suggested by the United Nations High Commissioner for Human Rights on the right to privacy in the digital age as a threshold for justifying state electronic surveillance [10].

Table 1: Example Standards of Proof

- an order for the liable party to discontinue harmful activity; or
- an order for the liable party to take some type of affirmative act (e.g., transferring ownership of property).

The principles of civil law are often crafted in an effort to redress negative externalities of behaviour in a modern economy. This makes civil law especially interesting in cyber security, as poor security in the development of ICT products and services is a sadly recurring negative externality that often falls short of criminal behaviour [11]. Policy makers hope that people who become aware that certain types of risk-taking carry an associated liability for resulting harm will alter their behaviour for the better.

A single act or series of connected acts can create liability simultaneously under both criminal and civil law. A hypothetical example in cyber security would include Alice making unauthorised access to Bob's computer which in turn causes Bob's LAN to fail. In this case, the state can prosecute Alice for the relevant crime (i.e., unauthorised access) and Bob can bring a civil legal action (i.e., negligence) seeking to establish that Alice is financially liable for harm caused. The two legal actions would normally be brought by two different persons (the state and Bob, respectively), contested in two separate tribunals, and subject to two different standards of proof as explained in Section 1.3.

2 Jurisdiction

[1, 12, 13]

Cyberspace enables persons located in different states to communicate with one another in a fashion that is unprecedented in history. Once-unusual international contacts and relationships have become commonplace. Those who face a potential threat of enforcement by a person in a foreign state must consider a few threshold questions before the relevant legal risk can be analysed: jurisdiction and conflict of law.

Jurisdiction describes scope of state authority and the mechanisms used by a state to assert power. Applicable law, or conflict of law, examines how to determine which state's domestic law will be applied to resolve certain aspects of a given dispute. This section of the knowledge area discusses jurisdiction. Conflict of law is addressed separately in the context of individual substantive headings of law.

Many of the principles concerning jurisdiction and conflict of law are not new. What has changed are the larger numbers of people who benefit from considering these principles now that persons are facing cross-border legal responsibilities at increased rates.

2.1 Territorial jurisdiction

The term 'jurisdiction' is often used in a rather informal manner to refer to a state, or any political sub-division of a state, that has the authority to make or enforce laws or regulations.[29] In this sense, the term is nearly synonymous with the territory of that state or its political sub-division. The purpose of this section, however, is to focus more specifically on the territorial extent of a state's power – its territorial jurisdiction.[30]

When reviewing legal risks from multi-state activities conducted via cyberspace, it may be helpful to consider three different aspects of jurisdiction: regulatory jurisdiction, juridical jurisdiction, and enforcement jurisdiction.

Regulatory jurisdiction describes the scope of authority claimed by a state to regulate the activities of persons or take possession of property. Law makers normally adopt laws for the purpose of protecting the residents of their home state and may declare their desire to regulate the actions of foreign-resident persons to the extent that such actions are prejudicial to home state-resident persons.

Juridical jurisdiction describes the authority of a tribunal to decide a case or controversy. The rules of such jurisdiction vary widely from tribunal to tribunal. In civil cases, courts usually demand a minimum degree of contact between the residential territory of the court and the property or person against which legal action is taken. Such minimum contact might involve obvious examples such as the presence of a branch office. It might be extremely minimal, indeed, resting upon little more than correspondence soliciting business from a resident of the court's territory.[31] In the context of criminal prosecutions, courts normally demand the physical presence of an accused before proceedings commence. Some states allow courts to make exceptions to this rule and are prepared to conduct a criminal trial *in absentia* if the defendant cannot be found within the territorial jurisdiction of the court.

Enforcement jurisdiction describes the authority of a state to enforce law. This is sometimes described as police power, power to arrest and detain, authority to use force against persons, etc. In civil matters, this may describe other methods used to project force over persons or property resident in a territory, such as seizing plant and equipment, evicting tenants from property, garnishing wages, seizing funds on deposit with a bank, etc. In practice, enforcement jurisdiction is limited by the ability of the state and its agents to project power over the objects of enforcement.[32]

2.2 Regulatory jurisdiction

It has long been commonplace for states to exert a degree of regulatory and juridical jurisdiction over non-resident persons who solicit business relationships with residents. A theory often espoused is that non-resident persons who remotely solicit or enter into business relationships with residents avail themselves of the benefits of the domestic market and, therefore, become amenable to the rules of that market. This principle long predates the Internet.

More controversial are cases where a non-resident person is not soliciting business from a state resident but may nonetheless be acting in a fashion which somehow harms state residents. Some of the best-known examples arise in competition law (a.k.a. anti-trust law). These cases follow a familiar pattern. A cartel of persons who produce commodities (e.g., bananas, aluminium, wood pulp, diamonds) outside of the state's territory, convene a meeting that also takes place outside the state's territory. In this meeting the cartel members conspire to fix the wholesale prices of a given commodity. This kind of offshore price-fixing conspiracy, which would be disallowed if it took place within the state's territory, eventually results in inflated prices inside the state as well. The only communication between the prohibited act (price fixing) and the state is the price inflation in the overseas (exporting) market, which in turn causes inflation of domestic (importing) market prices.

At the start of the twentieth century the notion of applying a state's domestic competition law to such overseas activity was considered wholly inappropriate [14]. The growth of international trade in the modern economy, however, lead to reconsideration. US courts decided in 1945 that extending regulatory jurisdiction to foreign price-fixing activity was justified due to the consequential harm to the domestic market and the sovereign interest in protecting the functioning of that market [15]. A substantially similar (if not identical) doctrine was announced in 1988 by the European Court of Justice when applying European competition law [16, 17]. Although these jurisdictional theories have been criticised, they are now exercised routinely.

States also claim regulatory jurisdiction over some actions taken by their own nationals while present in a foreign state even if no express 'effect' is claimed within the territory of the home state. Examples include laws prohibiting bribery of foreign officials [18] and laws against child sex tourism [19, 20]. States may also claim regulatory jurisdiction over violent acts committed against a state's own nationals outside of the state's territory by any person, especially in cases of terrorism.[33]

Instances where more than one state claims jurisdiction over a single act or occurrence are not uncommon. Claims of regulatory jurisdiction tend to be founded on notions of protecting the interests of a state and its residents. Some of the rules of jurisdiction have been adopted with a view to reducing instances where persons might face irreconcilable conflict between the mandates of two

states. Although such irreconcilable conflicts are less common than some might believe, they still arise from time to time. In cases where a person faces an irreconcilable conflict of mandates imposed by two states, the person is required to make hard choices. For businesses, these choices often involve changing business processes, structure or governance to avoid or limit the potential for such conflicts.

2.2.1 Regulatory jurisdiction over online content

Numerous court decisions around the world have confirmed the willingness of states to assert regulatory jurisdiction over actions where criminal or tortious content originates from outside of the state's territory, is transferred via the internet, and displayed within the state's territory. Examples of laws that have been enforced on this basis include copyright, defamation, gaming/gambling services, and state-specific subject matter prohibitions such as the prohibition against displaying or offering for sale Nazi memorabilia within France [1, 12, 13, 21].

These exercises of jurisdiction do not necessarily rest on the more attenuated 'effects doctrine' used in competition law. Courts seem willing to interpret domestic law in a fashion which asserts regulatory jurisdiction, and then to assert their own juridical jurisdiction on the basis that content is visible to persons within the state irrespective of the location of the server from which it originates. In this fashion, the offending act (e.g., copying, publishing, transmitting, displaying, offering for sale) is said to take place within the state asserting jurisdiction.

2.2.2 Regulatory jurisdiction over computer crime

States adopting computer crime laws often legislate to include cross-border acts. As a result, it is common for a state with such laws on their books to exercise regulatory jurisdiction over persons – no matter where they are located – who take actions directed to computer equipment located within the state. Similarly, persons who act while physically located within the state's territory are often caught within the scope of the criminal law when conducting offensive operations against computers resident in foreign states [22, 23]. Public international law most likely recognises as legitimate such exercises of regulatory jurisdiction (Tallinn 2.0 R.1-4, R.10 [9]).

When a hacker who is physically present in one state directs offensive activity to a computer in another state, that hacker may violate the criminal law of both states. If the relevant hacking activity does not constitute a crime in the first state for whatever reason,[34] it may still constitute a crime under the law of the second state where the target computer is located [23].

2.2.3 Regulatory jurisdiction and data protection (GDPR)

GDPR brought about a significant change in the territorial regulatory jurisdiction of European data protection law [24].

GDPR, in common with its predecessor 1995 legislation, applies first to any 'processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not' (Art. 3(1)). The term 'establishment of a controller' as used in EU data protection law generally, is extraordinarily broad when compared with other commonly understood legal principles. Creating or maintaining an establishment in the territory of the EU merely means the ability to direct business affairs or activities. This definition is not restricted by the usual niceties of corporate or international tax law. A holding company in the US, for example, can be deemed to have a personal data processing establishment in the EU through the non-processing activities of its wholly owned subsidiary [25]. Thus, legal persons who have no 'permanent establishment' or 'taxable presence' in the EU for purposes of analysing direct tax liability may nonetheless be deemed to be carrying out data processing in the context of an 'establishment' in the EU for the purposes of analysing GDPR liability.

GDPR now also asserts regulatory jurisdiction over the personal data processing activities of any person, anywhere in the world, related to offering goods or services to data subjects in the EU (Art. 3(2)(a)). Regulatory jurisdiction is believed to extend only to circumstances when the supplier volitionally offers such goods or services to data subjects in the EU.

Finally, GDPR applies to any person who monitors the behaviour of data subjects located in the EU, to the extent that this monitored behaviour 'takes place in' the EU (Art. 3(2)(b)). This heading of jurisdiction appears to have been motivated primarily by the emergence of services which monitor and analyse a variety of human behaviours including actions performed by persons using web browsers, or physical movement patterns exhibited by persons on the ground such as shopping behaviour.

Persons located outside the EU, who are nonetheless subject to the regulatory jurisdiction of GDPR because they offer goods or services to, or monitor the behaviour of, persons resident in the EU, are often required to appoint a representative in the EU (Art 27; Recital 80).

Interpreting the scope of GDPR's territorial jurisdictional can be difficult, especially given the rapid emergence of new forms of online services. The European Data Protection Board is expected to issue formal guidance in due course [26].

2.3 Enforcement jurisdiction

While it is relatively easy to imagine a state exercising broad regulatory and juridical jurisdiction over activities and controversies, more difficult questions arise with respect to enforcement jurisdiction: how a state practically enforces its rules.

As a general proposition, one state has no right under public international law to exercise enforcement jurisdiction within the territory of another state (Tallinn 2.0 R.11 [9]).[35]

This section considers some of the more common enforcement mechanisms used by states in a cyber security context. Enforcing the law tends to turn on three different mechanisms of state power: power over persons *in personum* jurisdiction), power over property (*in rem* jurisdiction), and requests or demands for international assistance addressed to other states.

2.3.1 Asset seizure and forfeiture generally

It is common to assert *in rem* jurisdiction over the property or other legal rights of an enterprise resident within a state's territory and amenable to that state's police powers. The state might seize such property in an effort to compel attendance at court proceedings, or eventually sell the property to meet the financial obligations of an absent person. Examples of objects seized for this purpose include immovable property such as office buildings or factories, movable property such as plant and equipment, trucks, maritime vessels, or merchandise in transit, and intangibles such as intellectual property or funds on deposit with a bank.

2.3.2 Seizure and forfeiture of servers, domain names, and registries

When a server located in a state is used to conduct activity that constitutes a crime in that state, seizing the server as an enforcement mechanism might be considered. Moving beyond the server, however, US law enforcement authorities have also used *in rem* jurisdiction for seizure and forfeiture of domain names where the domain TLD registry is maintained in the US. Actions for infringement of trademark rights have used similar *in rem* powers for domain name seizure and forfeiture. This is a potentially interesting enforcement tool in the US, especially as TLD registries administered and maintained from within the territory of the US include '.com', '.org' and '.net' [27, 28].

Similar *in rem* powers have been asserted by various states to regulate the administration of the ccTLD registry associated with their state, or to forcibly transfer the administration and operation of the ccTLD to a different in-state administrator [29].[36]

2.3.3 Territorial location of the right to demand repayment of bank deposits

Efforts to enforce laws that freeze or otherwise restrict depositor access to funds on deposit have raised difficult questions about the territorial scope of state enforcement authority. Asset freeze orders directed to enemy states or their citizens are not unusual, especially at times of international conflict.

A case highlighting this problem arose from the 1986 order issued by the United States mandating the freeze of assets held by the state of Libya. This order by the Reagan administration was historically unusual. In addition to mandating the freeze of money on deposit in the United States, it also ordered any US person who maintained effective control over any bank account anywhere in the world to freeze money on deposit in any of these global bank accounts.

The Libyan Arab Foreign Bank (a state-owned Libyan bank) took legal action against US banks in the courts of England demanding the repayment of deposits (denominated in US dollars) held in London branches. The resulting English court judgment makes for interesting reading, as the court discussed at length the extensive role of electronic funds transfer systems in international banking at that time. Having looked at the question, however, the dematerialised nature of funds transfers ultimately had almost no impact on the outcome of the case. The court held that money deposited with the London branch of a bank constitutes a legal right for the depositor to demand payment of that money in England [30, 31].[37]

In other words, a bank account may be conceptualised as being situated within the territory of the state in which the branch to which the deposit is made is located. This analysis continues to apply if the relationship is carried out entirely through online interactions, and indeed even if the depositor remains offshore and never attends the branch in person.

2.3.4 Foreign recognition and enforcement of judgments

A civil judgment issued by the court of one state may under certain circumstances be enforced by the courts of a friendly second state. This is normally achieved when the prevailing party transmits the judgment to the courts of the second state where the adverse party has assets, requesting enforcement of the judgment against those assets. Foreign recognition and enforcement of civil judgments is often granted under the principle of *comity*: a doctrine which can be expressed in this context as, 'We will enforce your civil judgments because, as a friendly state, we anticipate you will enforce ours.'[38]

A foreign court's willingness to enforce such civil judgments is not universal. Requests for civil enforcement are sometimes rejected for policy reasons. Nonetheless, this remains a relatively common mechanism in the context of judgments for money damages arising from many contract and tort disputes.

2.3.5 Extradition of natural persons

Criminal enforcement jurisdiction over natural persons normally proceeds on the basis of physical custody of the accused within the prosecuting state. If the accused is not present within the state, a traditional method of obtaining custody is to request extradition from another state [22]. Extradition is normally governed by bilateral extradition treaties, and is normally only allowed when the alleged criminal act constitutes a crime in both states (the requirement of dual criminality).

Extradition has a troubled history in cyber security. Extradition requests for accused cyber criminals might be denied by another state for a number of reasons: the lack of an extradition treaty between the two states, the lack of dual criminality for states where hacking is not a crime, public policy concerns over the severity of punishment to be imposed by the requesting state and general concerns over the health or welfare of the accused, are all reasons that have been cited for refusal to grant the extradition of persons accused of cybercrime [12].

2.3.6 The arrest of natural persons in state territory

It is normally straightforward for police officers to arrest persons present within their state's territory. When criminal suspects reside outside the state, officials are sometimes able to arrest a person when they subsequently appear in state – whether or not that state is an intended destination. In these cases, law enforcement officers can normally arrest the accused upon their arrival in state territory.[39]

State authorities can normally exercise the power of arrest on any seagoing vessel within the state's territorial waters, as well as vessels registered under the flag of the arresting state when in international waters. Additional maritime enforcement scenarios are possible [32].

2.3.7 Technological content filtering

Technological intervention can be adopted as a practical expression of state power – either by a state directly ordering such intervention, or by other persons adopting a technical intervention to avoid or limit liability.

Content filtering is merely one kind of technological intervention that can be used to enforce law or to reduce the risk of adverse enforcement activity. This approach fits generally within the concept explored by Lawrence Lessig and expressed with the phrase, 'code is law' [4].[40]

An enforcing state can direct an enforcement order to a person mandating that they filter content at the point of origination, whether the content is hosted on an in-state or out-of-state server [21]. Such an order carries with it the implicit or explicit threat that failure to implement the order could result in the use of other, more aggressive, enforcement mechanisms directed to in-state persons or property.

If an out-of-state person who originates or hosts offending online content from out-of-state infrastructure fails or refuses to filter it, the enforcing state might look to other technologically-based enforcement methods. A state might issue an order to in-state ISPs to block the in-state receipt of offending content [33]. Although such technical mechanisms are far from perfect (as is the case with any border enforcement technology), they may be sufficiently effective to accomplish the purpose of the enforcing state.

Filtering efforts are also initiated in the absence of specific state enforcement activity. Persons create and impose their own filters at point of origin to limit content transfers to states where filtered content might result in liability.[41] Filtering efforts can be conducted collaboratively between private and public sector actors.[42]

2.3.8 Orders to in-state persons directing production of data under their control whether held on domestic or foreign IT systems

States may also order state-resident persons to produce data under their control, irrespective of the territorial location of data storage.

Such orders are especially common under court procedural rules that govern disclosure (a.k.a. discovery) of potential evidence by the parties to a dispute. Those who find themselves party to a dispute that is subject to the jurisdiction of a foreign court must quickly become familiar with that court's rules of mandated disclosure. Courts normally do not feel constrained by the location of potential evidence – only that the parties to the dispute disclose it as required according to forum court rules.

More controversial are cases where a state, often in the context of a criminal investigation or intelligence gathering operation, demands the production of data under the control of a state-resident person who is not the target of (criminal) investigation or a party to the (civil) dispute.

An early example involved a previously secret program where the United States demanded lawful access to banking transaction records held by SWIFT. The orders to produce data were addressed

to US-resident SWIFT offices. Failure to comply with the US demands could have resulted in criminal prosecution of US-resident persons under US law. Complying with these demands, however, very probably constituted a violation of the data protection law of Belgium (SWIFT's headquarters), among others. News of the programme leaked in 2007 and created a diplomatic dispute between the US and Belgium (among others). This diplomatic issue was eventually resolved through negotiation and agreement concerning the scope of future investigatory operations [34].

Another well-known example involved a request made by an unknown agency of the US government under the Stored Communications Act. The government asked the court to issue an order to the Microsoft Corporation demanding the production of the contents of an email account maintained by Microsoft on behalf of an unnamed customer who was not resident in the US. A US court order was issued to Microsoft in the US, although the email account itself was maintained on a server in a data centre in Dublin, Ireland. US-resident staff of Microsoft had the technological ability to access the contents of the Dublin server, and the act of producing the requested data would have been technologically trivial. Microsoft asked the court to quash (invalidate) this order, generally on the grounds that the law did not authorise an order of this type with respect to data stored offshore.

After multiple skirmishes in the trial court, the US Court of Appeals (2nd Circuit) eventually quashed the order against Microsoft on the extremely narrow basis that the Stored Communications Act (adopted in 1986) did not expressly and unambiguously claim regulatory jurisdiction over data stored on equipment located outside the territorial United States [35, 36, 37].[43] This decision was appealed to the US Supreme Court. Following argument but before judgment, the US Congress in 2018 adopted the CLOUD Act. This amended the Stored Communications Act to bring data stored on foreign servers expressly into the regulatory jurisdiction of that Act, and the US government requested a replacement warrant under the revised law. The Supreme Court then dismissed the pending appeal without issuing a substantive judgment, as the new law had resolved any dispute about the intended scope of regulatory jurisdiction claimed by the US Congress [38].[44]

2.4 The problem of data sovereignty

The phrase 'data sovereignty' is sometimes used to struggle with the various jurisdictional demands outlined above. The extremely low technological cost of storing and then retrieving data outside the territory of a state, raises concerns about the number of states that might seek to compel disclosure of such data.[45]

Cloud services merely provide 'a *sense* of location independence' rather than actual location independence.[46] The location of a service provider's infrastructure and the location of persons who maintain effective control over that infrastructure are both important for understanding which states might be able to assert enforcement jurisdiction mandating some type of intervention with respect to such data [39].[47]

Users of cloud services have become increasingly aware that locating a data storage facility in any given state increases that state's opportunity to exercise enforcement jurisdiction over such facilities. Practitioners should also consider enforcement jurisdiction opportunities presented to a state when persons on its territory have technical or organisational ability to access data held on infrastructure physically outside that state. (See the discussion in Section 2.3.8) Enforcement risk can arise from the geo-location of data storage equipment, or the geo-location of persons able to access such data.[48]

Some states have responded to jurisdictional pressures by mandating the localisation of some types of data. Indeed, under its data protection laws the European Union has long imposed an EEA localisation requirement (in the form of a rule prohibiting export) for personal data although in practice there are multiple mechanisms available to enable exports from the EEA (see Section 4.6). Other states outside the EEA have imposed localisation requirements, for a variety of reasons [40, 41, 42, 43, 44].

Some states within the EEA have imposed single-state data localisation rules for certain types of sensitive data, prohibiting exports even to fellow member states of the EEA. Possibly in response to

this single state localisation trend, the European Union adopted a Regulation in 2018 that prohibits member state legal restrictions on the free movement of *non-personal* data within the Union. (I.e., the Regulation does not prohibit member states from adopting data storage localisation requirements for personal data.) This Regulation also includes multiple exceptions for member states who wish to impose localisation requirements for reasons of important public policy [45].[49]

3 Privacy laws in general and electronic interception

The concept of 'privacy' is both widely cited and challenging to articulate. This section addresses privacy in the sense described in the seminal nineteenth century article, 'The Right to Privacy' [46]. In this context, privacy has been described simply as the right to be free from intrusion by others into one's personal affairs or the 'right to be left alone'.

In the work of a cyber security practitioner, the issue of privacy most often arises in the context of electronic surveillance and related investigatory activity, which is the focus of this section. This area of law can be expected to continue to evolve quickly in response to new use cases enabled by cloud data processing services.

Data protection law is addressed in Section 4 and crimes against information systems are considered in Section 5. Most of these areas of law stem from or are related to privacy concepts.

3.1 International norms: foundations from international human rights law

Privacy is widely recognised internationally as a human right,[50] although not an absolute right. The right to privacy is conditional – subject to limitations and exceptions.

The 1948 Universal Declaration of Human Rights states at Art 12 that, 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. . . ' [47] Freedom from interference with privacy extends only to 'arbitrary' interference, which clearly contemplates the legitimacy of 'non-arbitrary' interference. Similar expressions, with similar qualifications, can be found in Article 8 of the European Convention on Human Rights [48] and again in Article 7 of the Charter of Fundamental Rights of the European Union[51] [49].

In the more narrow context of limiting government authority, the Fourth Amendment of the US Constitution adopted in 1791 states, 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants [authorizing search or seizure] shall issue, but upon probable cause. . . ' [50]. Again, this right is limited to protect only against such actions that are 'unreasonable'.

The application of these principles to intangible data evolved significantly during the twentieth century. In 1928, for example, the US Supreme Court interpreted the Fourth Amendment narrowly as protecting persons only from physical intrusion into their property [51]. Four decades later, after electronic communication had become a ubiquitous feature of everyday life, the Court changed its position and re-interpreted the Fourth Amendment to protect persons from unwarranted intrusion into electronic communications. The 1967 Court observed that laws like the Fourth Amendment are intended to 'protect people not places' [52]. The privacy right expressed in the European Convention on Human Rights has long been understood to apply to electronic communications [53]. By the early twenty-first century it appears to have become a widely accepted international norm that privacy rights (however they are interpreted) extend to intangible expressions of information as well as physical space [54].

While the principles described above are widely accepted in the international community, the interpretation and implementation of these principles remains subject to significant divergence. Some laws extend a general right of privacy into almost every situation, while others focus solely on limiting the power of the state to intrude into private affairs.[52]

A given person's expectation of privacy may vary by reference to the nature of their relationship with the party who seeks to intrude. For example, there tend to be few restrictions imposed by any state's

laws with respect to intrusion by a parent into the affairs of their minor children. By contrast, states vary significantly when considering when it is appropriate for employers to intrude into the affairs of their employees. In the latter context, the UN has published recommended approaches to the application of human rights in a business setting [55].

Expectations of privacy can also vary significantly between different societies. An intrusion viewed by one society as relatively innocuous and to be expected might be viewed by another society as a breach of human rights.

As persons rely on cloud services to manage increasingly intimate aspects of their personal lives, expectations of privacy over the variety of data processed using these systems will continue to evolve.[53] Policy makers, service providers, and civil society organisations, regularly seek to explain or to adjust expectations of privacy through education and advocacy.

An additional aspect of privacy relates to limits imposed upon the degree of permitted intrusion. In cases of state-warranted lawful interception, for example, warrants may be narrowly drawn to limit interception to named places, specified equipment, specified persons, or specified categories of persons.

Privacy laws often treat metadata differently from content data, usually based on the theory that persons have a lower expectation of privacy in metadata [56].[54] This distinction is increasingly criticised, and policy makers are under pressure to reconsider the nature of metadata given: (1) the private quality of some information disclosed by modern metadata such as URLs,[55] (2) the incredible growth in the volume and types of metadata available in the age of ubiquitous personal mobile data communications [56] and (3) the types of private information that can be inferred from metadata using modern data analysis techniques.[57] This area of law will likely undergo further evolution and revision.

3.2 Interception by a state

State intrusion into electronic communication for purposes of law enforcement or state security are often treated under specialist legal regimes that are highly heterogenous. There is broad agreement in public international law dating to the mid-nineteenth century that each state has the right to intercept or interrupt electronic communications in appropriate circumstances [57]. These principles continue to apply to cyberspace [9, 58].

As electronic communications (especially telephones) became commonplace and interception methods became more cost-effective in the 1960s and 1970s, a trend emerged to move state interception of communications activity away from informal or customary practice onto a more clearly regulated footing [53, 59]. Although legal governance processes and standards adopted to authorise state interception have evolved significantly, these legal processes and standards differ significantly from state to state. Some states require a prior examination of each request for state interception by an independent judicial officer; some delegate this decision-making authority broadly with limited oversight and others adopt mechanisms that fall anywhere between these extremes.

Although there does not yet appear to be any obvious international harmonisation of legal standards and procedures concerning lawful interception, there are examples of recommended practice for states that wish to place their legal procedures onto a robust and predictable foundation [60].

By contrast, some technical standards for facilitating lawful access (such as the ETSI LI series) have developed successfully on a multilateral basis [61, 62]. These technical standards make it possible for product and service developers to design lawful access technologies to a common multinational standard, while leaving substantive decision-making about their use in the hands of domestic authorities.[58]

Practitioners who work in a police or state security environment must become familiar with the rules that apply to their interception activity. Some state organisations employ large teams of lawyers dedicated solely to assessing the legality of various intelligence-gathering and investigation activities.

Those who work for communication service providers must also become familiar with obligations imposed on them by applicable laws to assist in state interception activity. This can prove especially challenging for multinational communication service providers, as they are normally subject to the regulatory jurisdiction of each state where their service is supplied. Service providers often localise responsibility for compliance with lawful interception by domestic authorities in each state where they supply services.

State regulations concerning lawful interception tend to impose a combination of obligations upon the providers of public communications services, such as:

- procuring and maintaining facilities designed to facilitate lawful interception within the service provider's domain (this obligation may be imposed under telecommunication regulation as a condition of telecommunications licensing, especially for those who operate in-state physical infrastructure such as PSTN operators);
- providing technical assistance in response to lawful interception requests; and
- maintaining the secrecy of the content of lawful interception requests, especially the identity of investigation targets.

Some states impose additional legal obligations to maintain secrecy over the existence, nature, or frequency, of lawful interception requests, the location or operation of interception facilities, etc. Communication service providers who wish to report publicly about the nature and frequency of state interception requests (a.k.a. transparency reports) must be careful to conduct this reporting in compliance with applicable law.[59]

As easy-to-use cryptographic technologies have become ubiquitous, and larger volumes of message traffic are transmitted as ciphertext, states conducting lawful access activity face increasing difficulty obtaining access to plaintext messages [59]. States have attempted to recover plaintext by using a variety of creative legal mechanisms including warrants for the physical search and seizure of end point devices and requests for technical assistance from device manufacturers or third-party analysts. These procedures are of variable effectiveness and remain subject to much debate [59]. Efforts to compel an end user to decrypt ciphertext or to disclose relevant passwords or keys also face a variety of legal challenges [63, 64].[60] Some states have adopted laws that specifically address compelled disclosure of plaintext or keys that enable decipherment.[61]

The emergence of virtual communication service providers (i.e., those who provide communication services via third-party infrastructure – or 'over the top' service providers) have created challenges for both states and service providers. These service providers remain subject to the jurisdiction of states in which their service is supplied, as states show a clear sovereign interest in services provided to persons within their territory.[62] States have, however, taken different approaches when choosing how and when to exercise jurisdiction over these providers. Enforcement actions by states against such persons have included orders to facilitate in-territory lawful interception at the risk of a variety of sanctions including: prohibiting the service provider from entering into business relationships with in-state residents, or ordering third-party state-resident service providers to block or filter such services at the PSTN or IP layer, thus making it inaccessible to (many or most) in-state residents. Changes in enforcement practices are likely as this subject continues to develop.

3.3 Interception by persons other than states

Laws concerning interception activity by non-state actors are also highly heterogenous.

Persons who provide public telecommunications services are often specifically restricted from intercepting communications that transit their own public service networks [36, 65]. This might be framed

legally as a restriction imposed only on providers of these public services, or a more general restriction limiting the ability of any person to intercept communications on public networks.

In many cases, efforts to intercept communications while transiting a third-party network will also constitute a crime under computer anti-intrusion laws. This was a significant motivating factor in the adoption of these laws (see Section 5).

The interception of communications by a person during the course of transmission over its own non-public network, such as interception on a router, bridge or IMAP server operated by that person on their own LAN, presents other challenges to analysis. This type of interception activity would not normally expect to fall foul of traditional computer crime legislation, as the relevant person is normally authorised to gain entry to the relevant computer (see Section 5). It might, however, be regulated generally within the same legal framework used to govern the interception of communications, although interception by an owner/controller on their own system is often treated more liberally [65]. Finally, in-house interception activity may also be limited by the terms of general privacy statutes or data protection laws (see Section 4).

3.4 Enforcement of privacy laws – penalties for violation

Enforcing a legal right of privacy brings a number of challenges. From an evidentiary perspective, a person whose privacy rights have been violated might never learn that a violation has occurred. Some legal rules serve, among other things, to redress this knowledge imbalance. These include breach notification requirements which reveal inappropriate disclosures of personal data to the effected person (see Section 4.7), criminal procedure rules that require the disclosure of prosecutorial evidence to the accused which in turn reveals intrusive investigatory techniques,[63] and civil procedure rules which require similar disclosures in civil legal actions (e.g., employment disputes).

Remedies available to persons whose privacy rights have been violated might include the ability to bring a tort action against the violator claiming monetary compensation (see Section 7.4). These individual tort remedies are a regular feature of data protection laws as well as various US privacy laws. The US criminal courts also employ an exclusionary rule prohibiting the introduction of evidence gathered in violation of the US Constitutional privacy rights of the accused [66].[64]

Finally, some violations of privacy – especially unwarranted interception of communications during the course of transmission on a public network or unauthorised intrusions into data at rest – are defined as and may be prosecuted as crimes [67].

4 Data protection

[12, 13, 68, 69]

Data protection law developed from a foundation of general privacy law. This generalisation can be a bit misleading, however, as data protection law has evolved to address a number of related issues that arise from modern data processing techniques that might not traditionally have been conceptualised as 'privacy'.

Data protection is of significant interest to cyber security practitioners, as it includes numerous obligations related to data security. This section will focus primarily on issues that recur in a security-related context. Data protection law is not, however, a generalised system of regulations that address every aspect of cyber security. The focus of these laws remain on specific principles that adopted to support individual rights in a data processing context.

Data protection law has developed primarily from European legislative initiatives. European Union law has been tremendously influential around the world through various mechanisms, including states seeking 'adequacy determinations' from the European Union, which enable exports of personal data, and private law contract requirements imposed upon non-EU resident data processors [70]. This

international impact continues to grow as the EU now expressly claims regulatory jurisdiction over personal data processing activity anywhere in the world that relates to EU-resident data subjects (see discussion in Section 2.2.3).

The foundational laws that define data protection obligations in the EU are Regulation 2016/679 – GDPR (EU-wide regulation applicable to most persons) and Directive 2016/680 (obligations to be imposed by member states in the context of state investigation or prosecution of crime) [24, 71].[65] This section primarily addresses obligations imposed by GDPR. Practitioners engaged by a state in conduct related to investigation or prosecution of crime must be aware of the modified obligations that apply to that activity as described by Directive 2016/680 and transposed into member state law [72, 73].

4.1 Subject matter and regulatory focus

EU data protection law exists to regulate acts of *data controllers* and *processors* in the context of *processing personal data*. Any such processing activity normally activates the application of data protection law. These terms are discussed in this section.

4.1.1 Data subject, personal data (and PII)

In data protection law, the terms 'personal data' and 'data subject' are defined concurrently:

> *personal data* means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (GDPR, Art 4(1))

Only natural persons, not legal persons, are data subjects. GDPR does not apply to personal data of deceased natural persons, although member states can individually adopt such protections if they wish (Recital 27).

Because the definition of data subject extends to persons who are *identified or identifiable*, data can incorporate personal data even when it includes no obvious information identifying a data subject. It is sufficient that a data subject is capable of being identified, by anyone, through analysing the data or by applying additional information known to any person - even if this additional information is unknown and inaccessible to the person controlling or processing data. Pseudonymised data remains personal data (Recital 26).

The Court of Justice of the European Union has held that a server log with IP address numbers incorporates personal data, as it remains possible for third parties (telecommunications service providers) to match static or dynamic IP numbers to individual customer premises and from there to a living person. This made some server log entries 'related to' a data subject [74]. The fact that the holder of the server logs did not have access to the IP number allocation or customer identification data was irrelevant.

As de-anonymisation and similar analysis techniques increase the capability to identify living persons from data that has no obvious personal identifiers, it becomes increasingly difficult to maintain data sets that are truly devoid of personal data.

Personal data is often confused in practice with 'personally identifiable information' (PII). This confusion arises because of the ubiquity of the term 'PII' in cyber security as well as significant variance in its definition.

Definitions and detailed discussions of PII are found in Section 4.4 of ISO/IEC 29100:2011, and Section 2.1 of NIST SP-800-122 [75, 76]. Although it is arguable whether the ISO and NIST definitions of PII are contiguous with the legal definition of personal data, both technical standards clearly conclude that data which contains no obvious personal identifiers may nonetheless constitute PII.

Complicating matters further, the phrase 'personally identifiable information' is used in a variety of US federal statutes and regulations, either without statutory definition, or with definitions specifically addressed to individual use cases.[66] In this specific context, some US courts have interpreted this phrase narrowly to include only obvious personal identifiers. Applying this narrow definition, some US courts have held that data such as MAC codes and IP numbers do not fall within the specified statutory definition of 'personally identifiable information' [77, 78, 79].[67] As explained above, these same identifiers often constitute 'personal data' as that term is defined in European law.

Irrespective of how one defines PII, European data protection law contains a clear and broad definition of 'personal data'. It is this definition of personal data, not PII, that triggers the application of European data protection law.[68]

4.1.2 Processing

In data protection law, the term *processing* is defined as:

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction (GDPR, Art 4(2))

Processing therefore incorporates almost any action one can imagine taking with respect to personal data.

4.1.3 Controller and processor

In data protection law, the term *controller* is defined as:

> the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law (GDPR, Art 4(7))

In data protection law, the term *processor* is defined as:

> a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (GDPR, Art 4(8))

These definitions make clear the relationship between controller and processor. A controller decides; a processor executes. In the history of data protection law, many policy makers originally believed that the most effective way to protect individual rights was to focus regulation on persons who operated and maintained computer equipment – processors. The focus was on the machine. As the

PC revolution changed our social relationship with computers, however, policy makers began to appreciate that the focus should be turned to persons in a position to command and control how the machines were used – controllers.

As between these two persons, Directive 95/46 tended to place the heaviest regulatory burden on controllers. Processors were advised that their obligation consisted primarily of following directions provided by controllers. There are many valid reasons for placing primary compliance responsibility on data controllers, especially because they are most often able to communicate and manage relationships with the relevant data subjects.

This regulatory distinction started to break down as cloud services became ubiquitous – especially SaaS. A typical SaaS provider might spend an enormous amount of time and effort designing their system and user interfaces, and then present the operational characteristics of that system to controller-customers in a service level agreement on a 'take it or leave it' basis. As a technical matter, the SaaS provider might be keen to demonstrate that they are acting only in the capacity of a processor and that their customers are acting as controllers – shifting the burden of assessing compliance to individual controllers. In the revisions to data protection law embodied in GDPR, policy makers have responded by generally increasing the regulatory responsibility of processors. Compliance responsibility under GDPR is now more evenly shared by controllers and processors, although their responsibilities depend upon their respective area of competence.

4.2 Core regulatory principles

Data protection law is built on a foundation of regulatory principles governing processing of personal data outlined in Article 5, being:

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy;
- storage limitation;
- integrity and confidentiality.

These core principles are well rehearsed and there are many published commentaries and guidelines available in forms accessible to practitioners to aid understanding [68, 80, 69, 81].

Practitioners should be especially alert to the presence of certain types of sensitive personal data in any system with which they are involved. Such data includes, 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation' (Art 9). Sensitive personal data triggers a series of additional protections and generally increased levels of regulatory scrutiny, as improper use of such data often presents a disproportional risk to the interests of the data subject.

The topic of 'consent' in data protection law is worth a brief comment, as it remains a subject of some confusion. As a threshold matter, data subject consent is not always required when processing personal data. There may be multiple lawful grounds for processing personal data other than consent depending upon context. If data subject consent is required, however, data protection law sets a very high bar that this must be 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies

agreement to the processing of personal data relating to him or her' GDPR Art 4(11). A series of conditions that apply to consent are set out in GDPR Art 7 (and Art 8 relating to children's consent).

4.3 Investigation and prevention of crime, and similar activities

Practitioners engaged by a state benefit from certain reductions in data protection obligations when processing personal data related to criminal investigation and prosecution. These reduced obligations are described in general in Directive 2016/680 and then transposed into member state law.

Practitioners who conduct activities with similar goals, but are not engaged by a state, remain subject to GDPR. In this context, however, GDPR makes it clear that purposes such as fraud prevention constitute a legitimate interest of data controllers (Recital 47). GDPR also provides member states with the option to adopt in their domestic laws reduced data protection obligations for non-state actors when conducting activities designed to prevent, investigate, detect, or prosecute crime, etc. (GDPR, Art 23) [82] at s.15 and Sched 2.

4.4 Appropriate security measures

Data protection law imposes an obligation on controllers and processors to 'implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk' associated with processing personal data (GDPR, Art 32(1).) This security principle is a long-standing feature of data protection law.

The obligation clearly encompasses both technical measures as well as human management and oversight (i.e., 'organisational measures'). Compliance requires that both components are appropriate. Compliance requires a consideration of the state of the art and an assessment of costs of various measures in comparison with risks presented. Assessing this obligation to take appropriate security measures might therefore be aided by analogy with the law of negligence which presents various frameworks to assess 'reasonable' care (see discussion in Section 7.1.2).

GDPR has expanded significantly the discussion of security measures to provide examples of measures that might assist in creating appropriate security. This includes many past practices that developed organically such as pseudonymisation and encryption of personal data, assuring ongoing confidentiality, integrity, availability and resilience of systems, and robust incident recovery plans. To be clear, GDPR does not expressly mandate encryption of all personal data. It simply highlights encryption as a technical measure that can be adopted to enhance security. As encryption methods or other security technologies become standardised and costs fall, however, it becomes increasingly difficult to justify why such technologies are not adopted.

Organisational methods used to protect the security of personal data extend to contract obligations with supply chain partners and others. (See also the discussions in Sections 4.6.2 and 6.2)

Although security certification or compliance with security codes of practice might help to prove appropriateness of security measures, these certifications are not dispositive (Art 32(3)).

4.5 Assessment and design of processing systems

Sometimes, the most effective way to prevent violations of data protection law is to design a system that minimises the ability of persons to take inappropriate action. GDPR, therefore, has adopted an obligation to implement data protection strategies by design, and by default. As with the general security principle, this obligation extends to both technological and organisation measures and is assessed on a risk balancing basis. This obligation arises at the planning phase, before processing commences, as controllers are required to consider this issue 'at the time of determining the means of processing' (Art 25).

If a new personal data processing activity presents significant risk of harm to data subjects, especially in the context of developing or migrating to systems that process large volumes of data, the controller

is required to undertake a data protection impact assessment (Art 35; Recital 91, et al.). If the assessment reveals significant risks, the controller is further required to consult with the relevant supervisory authority about the proposed processing activity (Art 36).

4.6 International data transfer

European data protection law imposes a general prohibition on the transfer of personal data to any state outside the European Economic Area or to any international governmental organisation (Art 44). Such transfers remain commonplace, however, when enabled by an appropriate export compliance mechanism.

4.6.1 Adequacy determinations and Privacy Shield

Transfers of personal data can be made to territories in accordance with an adequacy decision: a finding by the European Commission that the receiving territory (or IGO) has established adequate legal protections concerning personal data (Art 45). The process of obtaining an adequacy decision is instigated at the request of the proposed receiving state and often requires years of technical evaluation and diplomatic negotiation [70].

Adequacy determinations fall into two categories: decisions that a receiving territory's laws are generally adequate to protect personal data, and decisions that a receiving territory's laws are adequate provided that special conditions are met. Decisions concerning Canada and the United States both fall into the second category. In the case of Canada, adequacy is only assured with respect to transfers to the commercial for-profit sector, as the relevant Canadian laws do not apply to processing by governments or charities.

The US adequacy determination has a difficult history. The US has nothing like the EU's generalised legal protections concerning processing personal data. To enable transfers of data, the US and the EU have negotiated specific agreements to support an adequacy finding. This agreement enables most US businesses, if they wish, to opt in to a regulatory system that provides adequacy. This regulatory system is then enforced by agencies of the US state against opted-in US businesses. The original system, Safe Harbour, was invalidated by the European Court of Justice in October 2015 in the Schrems case [83]. It was quickly replaced by the EU-US Privacy Shield regime in 2016, which operates in a fashion similar to Safe Harbour with enhanced protections for data subjects.

4.6.2 Transfers subject to safeguards

Transfers are also allowed when appropriate safeguards are put into place (Art 46). The most common safeguards normally encountered are binding corporate rules, and approved data protection clauses in contracts between exporters and importers.

Binding corporate rules are governance procedures normally adopted by multinational enterprises in an effort to demonstrate to data protection authorities that they will comply with data protection principles (Art 47). To be effective for data transfer compliance, such rules must be approved by relevant public authorities. This can take years to negotiate. While such rules were originally developed as a tool to enable sharing of personal data among the members of a multinational data controller enterprise that operates both inside and outside the EEA, they have more recently been adopted by non-resident cloud service providers as a compliance tool to facilitate business from customers in the EEA. Practitioners may be called upon to assist in drafting or negotiating binding corporate rules, as they have a significant impact on IT services, security architectures and governance procedures.

Approved contract clauses are simply contract obligations between a data exporter and importer that serve to protect the interests of data subjects. They can be either standard clauses approved for use by the Commission, or special clauses submitted to the relevant authorities for prior approval (Art 46(2)(c)-(d) & 46(3)(a)). Although the Commission-approved clauses are standardised, to be effective

the parties to the relevant contract are required to incorporate a significant amount of operational detail about the nature of the personal data to be transferred, the purposes of the data processing to be undertaken, etc.

4.6.3 Transfers pursuant to international mutual legal assistance treaty

Transfers of personal data that are otherwise prohibited by GDPR can be made in circumstances such as requests for assistance by a foreign state police agency pursuant to the terms of a mutual legal assistance treaty (Art 48). Such transfers are addressed specifically in Directive 2016/680, Art 35-40.

4.6.4 Derogations allowing transfers

In the absence of any other mechanism allowing a transfer, exports from the EEA are still allowed under certain limited circumstances such as:

- the data subject provides knowing informed express consent to the transfer;
- the transfer is necessary in order to perform a contract with the data subject, or a contract with a third party adopted in the interests of the data subject;
- the transfer serves an important public interest;
- the transfer is connected to the pursuit or defence of a legal claim; or
- the transfer is necessary to protect the life or welfare of the data subject, who is physically unable to consent.

These derogations (Art 49) are meant to be interpreted narrowly, and the European Data Protection Board has issued guidance on the interpretation and application of these measures [84].

4.7 Personal data breach notification

Laws mandating the notification of personal data breaches to data subjects[69] began to emerge in both the EU and the US around the turn of the twenty-first century [85, 86]. In a pattern that is curiously the reverse of the development of data protection laws generally, EU notification requirements arose first in narrowly defined subject matter areas while US states (beginning with California) imposed a more general duty to notify effected persons of personal data breaches. By 2010, 46 US states had adopted legislation mandating some form of personal data breach notification to effected persons [87].

GDPR marked the emergence in Europe of a general duty placed on processors and controllers of personal data to make certain notifications following a 'personal data breach', which is defined as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed' (Art 4(12)). Thus, events as diverse as personal data exfiltration, the unauthorised modification of personal data and ransomware can all constitute personal data breaches.

A processor is first required to notify the circumstances of a breach to the relevant controller 'without undue delay'. The controller is then required to notify the relevant supervisory authority of the breach 'without undue delay and, where feasible, not later than 72 hours after having become aware of it' (Art 33(1)-(2)). The content of the notice is set out in Art 33(3). There is a limited exception to the controller's duty to notify a supervisory authority if the breach is 'unlikely to result in a risk to the rights and freedoms of natural persons'. Whether or not notified to the supervisory authority, the controller

is required to document all such breach events and these records are subject to periodic review by the supervisory authority.

If such a breach is 'likely to result in a high risk to the rights and freedoms of natural persons', then the controller is required to communicate the circumstances of the breach to the relevant data subjects without undue delay (Art 34(1)-(2)). Communication to the data subjects can be avoided if the controller has implemented methods that limit the harm that might be caused by such a breach, such as encrypting data that was then exfiltrated as ciphertext. While such ciphertext remains personal data for legal purposes, the encrypted state of the data reduces the potential harm to data subject to some degree (depending upon the type of encryption, etc.) This ability to avoid communication to data subjects when harm is unlikely is a useful feature of GDPR. Many US state notification laws originally demanded notifying data subjects irrespective of the relevant risks presented by the breach.[70] Supervisory authorities retain the right to compel communication to data subjects about the breach if they disagree with the controller's risk assessment.

4.8 Enforcement and penalties

Egregious violations of data protection law can be prosecuted as crimes under member state domestic law. Relevant actions can be prosecuted simultaneously as crimes against information systems (see Section 5) [88].

Data protection laws also enable data subjects to bring tort claims for violation of data protection rights. Such claims implicate the risk of vicarious liability for employee misdeeds, especially if a large group of data subjects are able to bring a claim as a group or class. (See the discussion of the *Morrisons* case at Section 7.5.1)

Public enforcement authorities are also given powers to serve enforcement notices, demanding changes in processing behaviour to achieve compliance with the law (Art 58.) In particularly egregious cases, public authorities might serve a notice prohibiting large categories of processing activity. Breaching such an enforcement notice is an independent cause for more severe enforcement action.

Historically, civil or administrative fines imposed by public authorities for violation of data protection law were perceived in some member states as relatively minor. The disparity in approach among member states to data protection law was a motivating factor for the adoption of the original 1995 Directive and it tended to increase data protection rights in most member states. Following the 1995 Directive, larger fines started to emerge as state authorities began to increase enforcement pressure. By the time GDPR was adopted in 2016, administrative fines in the region of €500,000 were not uncommon for significant violations of the law.

One the most-discussed features of GDPR concerns the authority granted to impose large administrative fines (Art 83). Violations of some of the more procedural or operational requirements of GDPR, including the requirement to adopt appropriate security measures, can incur administrative fines of up to €10,000,000, or 2% of an undertaking's annual worldwide turnover, whichever is greater. Violations of more fundamental principles of GDPR, such as failure to respect the rights of data subjects, processing personal data without lawful authority, or exporting data in violation of the law, can incur administrative fines of up to €20,000,000, or 4% of an undertaking's annual worldwide turnover, whichever is greater. Authorities are instructed to calculate fines at a level to make them 'effective, proportionate and dissuasive' in individual circumstances. GDPR lists a number of both mitigating and aggravating factors for consideration when setting these fines that are worth closer study (Art 83(2)).

The emergence in GDPR of the potential for 'eight figure' and 'nine figure' fines, together with the increased scope of territorial jurisdiction, instantly promoted data protection law into the category of a significant risk to be assessed and managed at senior leadership levels – a position that this law had rarely occupied prior to these changes. Some persons who provide online information services from outside the EU (who presumably fear that their business models are not compatible with GDPR

compliance) responded by withdrawing from the European market by using geographic filtering mechanisms (see Section 2.3.7). Other offshore service providers have embraced the change and worked to comply with the rules (presumably as they value their ongoing contact with the European market).

In July 2019, the Information Commissioner's Office of the United Kingdom issued two notices of their intention to issue large fines under GDPR: a proposed fine of GB£183.39 million to British Airways[71] and a proposed fine of GB£99.2 million to Marriott International, Inc.[72] At time of writing, both companies have signalled their intention to contest the fines.

5 Computer Crime

[22]

The term 'cybercrime' is often used to identify three different categories of criminal activity: crimes in which cyberspace infrastructure is merely an instrumentality of some other traditional crime (e.g., financial fraud), distribution of criminal content (e.g., pornography and hate speech), and crimes directed against cyberspace infrastructure itself (e.g., unlawful intrusion into a computer system).

This section is addressed solely to the last category, computer crimes or crimes against information systems. These tend to be of concern as they are of interest to those who work for state enforcement authorities, as well as those who manage cyber security risk, research cyber security technologies, and develop cyber security products and services.

Although some practitioners are engaged by states in the investigation and prosecution of crimes where cyberspace is an instrumentality of crime, it is difficult to draw out generalisable statements about those crimes that remain useful in a multinational context. Similarly, crimes based on message content are treated very differently by states, as these laws are borne of widely diverging social opinion about what constitutes 'illegitimate' content.

5.1 Crimes against information systems – introduction

In the 1980s and 1990s, many states confronted the problem that an emerging set of anti-social behaviours related to cyberspace infrastructure were not clearly identified as crimes.[73]

The UK Parliament responded by adopting the Computer Misuse Act 1990, which defined a series of computer-related criminal offences. This law has been subsequently amended from time to time [89].

In 1984, the US Congress adopted the Computer Fraud and Abuse Act, which has also been regularly amended [90]. Individual US states have also adopted state criminal laws which can be used to prosecute computer crime.[74]

Similar laws have been adopted by many, but not all, states around the world. The Council of Europe Convention on Cybercrime (a.k.a. the Budapest Convention) is a multilateral treaty which has had a significant impact on harmonising computer crime laws [91]. The Convention opened for signature in 2001, and as of June 2019 had been signed and/or ratified by more than 45 member states of the Council of Europe and more than 18 non-European states including Canada, Japan and the US [92].

In 2013, the European Union adopted Directive 2013/40. This mandates that member states modify their criminal laws to address commonly recognised computer crimes which the Directive describes as crimes 'against information systems' [23]. This introductory section on crimes against information systems is influenced by the taxonomy adopted by the Budapest Convention and is reflected in Directive 2013/40.

5.1.1 Improper access to a system

Improper system access laws criminalise the act of accessing a system without the right to do so, colloquially known as hacking.[75] (Directive 2013/40 at Art 3.) The UK Computer Misuse Act 1990 at

s.1, for example, defines as criminal an action by a person which causes a computer to perform an act with the intent to secure access to any program or data [93]. Thus, the act of entering a password into a system without authorisation in an effort to access that system constitutes a crime under the UK statute whether or not the access is obtained successfully.

5.1.2 Improper interference with data

Improper system interference with data laws criminalise the act of inappropriately 'deleting, damaging, deteriorating, altering or suppressing' data. (Directive 2013/40 at Art 5.) These laws can be used to prosecute actions such as release or installation of malware, including ransomware.

5.1.3 Improper interference with systems

Early computer crime laws tended to focus on the act of intrusion into a computer system, or improperly modifying the contents of those systems. With the emergence of DoS and DDoS attacks, some of these early criminal laws were found to be inadequate to address this new threatening behaviour.

These laws now more commonly include a prohibition against acts that cause a material degradation in the performance of an information system. (Directive 2013/40 at Art 4; Computer Misuse Act 1990 at s.3, as amended in 2007-08.)

5.1.4 Improper interception of communication

Often as a corollary to various rights of privacy, many legal systems define the act of wrongfully intercepting electronic communications as a crime. (Directive 2013/40 Art 6.) The rules and penalties tend to be most restrictive in the context of intercepting communications during the course of their conveyance on public networks. This subject is discussed in Section 3.

5.1.5 Producing hacking tools with improper intentions

Many states also define as crimes the production or distribution of tools with the intention that they are used to facilitate other crimes against information systems. (Directive 2013/40, Art 7; Computer Misuse Act 1990, s.3A.) These laws can create challenges for those who produce or distribute security testing tools, as discussed in Section 5.5.

5.2 *De minimis* exceptions to crimes against information systems

Some laws may limit the definition of computer crime to acts which are somehow significant. Directive 2013/40, for example, only mandates that member states criminalise acts against systems 'which are not minor' (Art 3-7). The concept of a 'minor' act against a system is discussed in Recital 11 to the Directive, which suggests that states might define this by reference to the relative insignificance of any risk created or damage caused by the given act [23].

This type of *de minimis* exception to the definition of computer crime is far from universal. EU member states remain free to criminalise such *de minimis* acts. At the time of writing, the UK legislation contains no such *de minimis* exception.[76]

The very idea of a *de minimis* exception to crimes against information systems raises a recurring debate over the nature of the harm that these types of laws seek to redress. It is not always clear how to assess the relative damage or risk caused by any given act against information systems. For some criminal acts such as remote intrusion into a chemical plant industrial control system the risk presented or harm caused is clear to see, as the attack is concentrated against a single and volatile target. In others, such as controlling the actions of a multinational botnet comprising tens of thousands of suborned machines, the risk created or harm caused may be widely diffused among the bots and more difficult to quantify.[77]

5.3 The enforcement of and penalties for crimes against information systems

States normally have absolute discretion to decide whether or not to investigate alleged crimes. Having investigated, states normally have absolute discretion regarding the decision to prosecute a criminal matter.[78] Some states have set out guidance to explain how this discretion is exercised [94].

Penalties for committing a crime against information systems vary widely. In criminal cases custodial sentences are often bounded in law by a maximum, and occasionally by a minimum, length of term. Within these policy-imposed limits judges are usually given a wide degree of discretion to decide an appropriate sentence.

Under the UK Computer Misuse Act, for example, a custodial sentence for the crime of improper system access is normally limited to a maximum of two years, while the crime of interfering with data or system integrity is normally limited to a maximum of five years. Prosecution and sentencing history both suggest that actual sentences issued under the UK legislation for these crimes are rarely, if ever, this severe. By contrast, in the US, both federal and state laws have consistently provided for longer maximum custodial sentences of 20 years or more for unlawful intrusion or unlawful interference with data.

The question of appropriate punishment for crimes against information systems remains the subject of review and debate. The emergence of the Internet of Things arguably increases the risk that these crimes might pose to life and property.[79] EU Directive 2013/40, for example, requires that member states provide for the possibility of longer custodial sentences when attacks are directed against critical national infrastructure or when they actually cause significant damage (Art 9(b)-(c)). The UK amended its Computer Misuse Act in 2015 (s.3ZA) to increase the maximum available custodial sentence if criminals are proven to have created significant risk or caused serious damage. Such a person could now be subjected to a maximum custodial sentence of 14 years. In cases where the criminal act causes (or creates significant risk of) serious damage to human welfare or national security, the maximum custodial sentence under UK law increases to life imprisonment (s.3ZA(7)).

Arguments continue over appropriate punishments for crimes against information systems. This debate is complicated by difficulties in understanding or quantifying the degree of risk or the degree of harm caused by these criminal acts. (See the discussion in Section 5.2.)

5.4 Warranted state activity

When actions related to investigation of crime or in defence of state security are conducted with state authorisation such as a warrant, the person using the warranted technique is often expressly exempted from that state's criminal liability for intrusion into information systems to the extent that the intrusion conforms with expressly warranted activity.

An example can be found in the UK's Investigatory Powers Act 2016, which holds that certain activity conducted with lawful authority under the terms of that Act are 'lawful for all other purposes' [65] in ss.6(2)-(3), 81(1), 99(11), 176(9), 252(8). In other words, actions in compliance with a warrant issued pursuant to the 2016 legislation will not constitute a crime against information systems under the Computer Misuse Act 1990 etc.[80]

State-sponsored acts of remote investigation into cyberspace infrastructure located in foreign states are considered in Section 12.4.

5.5 Research and development activities conducted by non-state persons

Those who research cyber security issues and develop security products and services outside of the domain of state-sponsored activity can face difficulties if their planned activities constitute a crime against information systems. Examples that may lead to difficulties include:

- uninvited remote analysis of security methods employed on third-party servers or security certificate infrastructures;
- uninvited remote analysis of third-party WiFi equipment;
- uninvited analysis of third-party LAN infrastructure;
- invited stress testing of live WAN environments, to the extent that this degrades third party network performance;
- analysing malware and testing anti-malware methods;
- analysing botnet components and performance;
- producing or distributing security testing tools; and
- various covert intelligence-gathering techniques.

With respect to testing tools specifically, the law tends to criminalise production or distribution only when the state can prove an intent to facilitate other violations of the law. This criminal act may have less to do with the operational characteristics of the testing tool than the subjective intention of the person who is producing or distributing it.[81]

In some states, researchers might be able to demonstrate a lack of criminal responsibility for these acts under some type of *de minimis* exception, if one is available (see the discussion in Section 5.2).[82]

State law makers sometimes rest on the belief that 'legitimate' researchers will be saved from criminal liability as a result of state discretion to refrain from investigating or prosecuting *de mimimis* criminal acts, judicial or jury intervention to find accused parties not guilty, or if found guilty, through the imposition of only a token punishment. This situation is rather unsatisfactory for practitioners who attempt to assess potential criminal liability arising from an otherwise carefully risk-managed research or development effort.[83]

Even if practitioners find appropriate exceptions under relevant laws concerning crimes against information systems, they must also be careful to consider whether their actions would constitute crimes under other laws such as generalised privacy or data protection laws.

5.6 Self-help disfavoured: software locks and hack-back

'Self-help' refers to the practice of attempting to enforce legal rights without recourse to state authority. A routinely cited example is the re-possession of movable property by a secured lender from a borrower in default of payment of obligations. (For example, repossessing an automobile.)

Public policy is generally suspicious of self-help mechanisms, as they involve non-state actors exercising powers normally considered to be the exclusive province of the state. Laws that enable such actions often impose multiple conditions that limit the actor. In the context of cyber security, practitioners have occasionally designed or adopted methods that might be classified as self-help.

These actions come with the risk of potentially violating criminal law. Persons pursuing these strategies should also remain aware of potential tort liability (see Section 7).

5.6.1 Undisclosed software locks

Various technologies serve to limit the use of software. Implementing a system that clearly discloses to a user that its operation requires the prior entry of a unique activation key is normally non-contentious, and is actively encouraged by certain aspects of copyright law (see Section 8.2.1). Similarly, providers of software as a service usually do not face any sanctions when suspending access to a customer who terminates the service relationship or fails to pay their service fees.[84]

Problems arise when a supplier (for whatever reason, including non-payment of promised license or maintenance fees) installs a lock mechanism into a software product after the fact without customer agreement. Also problematic are instances where software sold as a product contains an undisclosed time-lock device which suspends functionality in the event of non-payment. These types of undisclosed or *post-facto* interventions have a history of being prosecuted as crimes against information systems and are otherwise criticised as being against public policy [95, 96].

5.6.2 Hack-back

Hack-back is a term used to describe some form of counter-attack launched against cyberspace infrastructure from which an attack appears to have originated. This strategy is often considered in the context of an attack which originates in a different state, and cooperation from foreign law enforcement is deemed unlikely or untimely. Hack-back actions might consist of a DoS attack, efforts to intrude into and disable the originating infrastructure, or others.

Hack-back activity normally falls squarely within the definition of crimes against information systems and can be prosecuted as such by the state where the person conducting the hack-back is located, the states where the machines used to conduct the hack-back are located, or the state of the hack-back target. In addition to the risk of criminal prosecution, a hack-back (if sufficiently aggressive) could serve as the basis under international law for the state of the hack-back target to take sovereign counter-measures against the person conducting the hack-back or against other infrastructure used to conduct the hack-back operation – even if the hack-back itself is not directly attributable to the infrastructure host state (see Section 12).

Many have debated adopting exceptions in law specifically to enable hack-back by non-state actors [97, 98, 99]. These types of proposed exceptions have not yet found favour with law makers, and hack-back by non-state actors is generally considered a crime by those states that have adopted laws criminalising attacks on information systems.

6 Contract

[12, 13, 100]

Contract is civil legal concept that describes a (notionally) volitional relationship between two or more parties. One extremely broad definition of contract is simply, 'a promise that the law will enforce' [100].

Unfortunately, the word 'contract' is often used colloquially to describe a communication that embodies and expresses contractual promises (e.g., a piece of paper, email, or fax). This confusion should be avoided. A contract is a legal relationship, not a piece of paper. In some circumstances, applicable law may exceptionally impose a requirement that some contract obligations must be embodied in a specified form (see Section 10).

This section will discuss a few contract topics of recurring interest to cyber security practitioners.

6.1 Online contracts: time of contract and receipt of contractual communication

The definition of 'contract' above immediately begs a follow-up question: how does one distinguish a legally enforceable promise from other types of communication? Although different legal systems have varying approaches to defining a contract, the elements required by law can be classified into two categories: sufficiency of communication, and indicia of enforceability.

As an example, under the law of England a contract usually exists only when the parties have communicated an offer and an acceptance (collectively constituting sufficiency of communication), supported by consideration and an intention to create legal relations (collectively constituting indicia of enforceability).

Sufficiency of contract communication is a recurring issue when designing and implementing online transaction systems. Understanding the precise time when a contract comes into existence, the so-called contractual trigger, [13][c18] [12][c6] is important in risk-managing the design of online transaction systems.[85] Prior to the existence of a contract the parties generally remain free to walk away. Post-contract, however, the parties are legally bound by promises made.

System designers should consider four successive moments in the contract communication process:

1. the time at which Alice transmits her offer[86] to Bob;
2. the time at which Bob receives Alice's offer;
3. the time at which Bob transmits his acceptance to Alice;
4. the time at which Alice receives Bob's acceptance.

Most common law systems would, by default, place the time of contract formation for online transactions into the last of these four times – the moment that Alice receives Bob's acceptance.

Practitioners are urged not to conflate these four distinct moments in time, even when they appear to be instantaneous. System designers should consider the impact of a lost or interrupted transmission and, accordingly, technical design should be carefully mapped onto relevant business process.

A perennial question with online systems concerns the previse point in time at which it can be said that Alice or Bob has 'received' a communication. The European Union attempted to address this in Article 11 of the Electronic Commerce Directive 2000 [101]. This mandates adoption of a rule that 'orders' and 'acknowledgements' of orders[87] are generally deemed to have been received at the moment they become accessible to the receiving party (e.g., when the acceptance is received in Alice's online commerce server log or Bob's IMAP file).[88] This rule can be varied by contractual agreement in B2B commerce systems.

Differences in approach are worthy of investigation depending on the states where system users may be located, and the relative value of transactions supported.

6.2 Encouraging security standards via contract

Contracts can serve as a mechanism to encourage the implementation of security standards. This can arise in a wide variety of contractual relationships.

6.2.1 Supply chain

A common contract technique is to incorporate terms within a procurement agreement that attempt to mandate some form of compliance by a supply chain partner with specified security standards: whether published standards such as ISO 27001, or *sui generis* standards adopted by the contracting parties. Although these contract terms can take many different legal forms (e.g., warranty, representation, undertaking, condition, mandate to produce evidence of third-party certification, access and audit rights etc.) the general principle is that these contract terms have become a common mechanism that is used in an attempt to influence the security behaviour of supply chain partners.

The value of these clauses in managing supply chain behaviour, however, is worth a closer examination. Let us consider the risk-weighted cost to a contracting party when breaching the terms of such a clause. In a legal action for breach of contract, the enforcing party normally remains responsible for proving the breach caused financial harm, as well as the quantum of financial harm suffered by the enforcing party as a result of the breach. In the case of a failure to comply with an obligation to maintain a third-party security certification, for example, it might be difficult or impossible for the enforcing party to prove that any financial harm flows from such a breach.

A sometimes-overlooked value of these contractual clauses arises well before the agreement is made. The process of inserting and then negotiating these clauses can operate as a due diligence technique. A negotiating party obtains information about the maturity and operational capability of the proposed supply chain partner during negotiations.

6.2.2 Closed trading and payment systems

Many high-value or high-volume electronic trading or payment platforms[89] require persons to enter into participation contracts prior to using the platform. These systems may be generally referred to as 'closed' systems: they constitute a club that must be joined contractually to enable members to trade with one another. These membership contracts typically adopt comprehensive rules concerning forms of communication, connected equipment, and the timing for finality of transactions. They also typically specify the adoption of certain security standards, authentication protocols, etc. The membership contract is thus a private law mechanism that is used to enforce certain security standards among the members. (See also Section 10.2.)

Breaching the terms of the membership contract might jeopardise the subject matter of the agreement itself – the finality of trades or the ability to collect payment. As an example, a merchant collecting payment via payment card who fails to comply with the authentication procedures mandated by its merchant acquirer contract might face a loss of payment for a transaction even though it has delivered (expensive) goods into the hands of a person who has committed card fraud. Faced with such drastic financial consequences, the contracting parties may work exceptionally hard to meet the mandated authentication standards.

Perhaps the most well-known example of a widespread standard implemented using contract is PCI-DSS adopted by the payment card industry. Failure to comply with this standard puts at risk a party's ability to receive payment. While there is some debate about the degree to which this standard has been effective, it is difficult to deny that it has had some impact on raising the standard of security practices employed by many merchants when handling card transaction data – especially those who previously seemed to approach the subject with a cavalier attitude.

6.2.3 Freedom of contract and its limitations

When considering using a contract as a means of regulating security behaviour, one must consider that the law can and does interfere with or otherwise limit the enforceability of some contract terms.

When considering PCI-DSS standards, for example, the US Fair and Accurate Credit Transactions Act of 2003 [102] in Section 113 mandates specific truncation rules concerning payment card numbers displayed on printed receipts provided at the point of sale.[90] Thus, merchants subject to US law must consider these public law requirements as well as PCI-DSS, and those who wish to modify the PCI-DSS standards should do so in a manner that is sympathetic to the external requirements imposed on these merchants by US law.

In the case of funds transfer services, public law also establishes a framework to balance the rights and responsibilities of providers and users of payment services which includes considering the adequacy of authentication mechanisms. Examples can be found in Articles 97 and 4(30) of the EU Second Payment Services Directive (PSD2), as implemented in the laws of member states [103], and Article 4A §202 of the Uniform Commercial Code, as implemented in the laws of US states [104].

Limitations on the freedom of parties to deviate from public law norms in contract are further discussed in Sections 6.3 and 6.4.

6.3 Warranties and their exclusion

The term 'warranty'[91] describes a contractual promise concerning the quality or legal status of deliverables, the adequacy of information provided by a party, the status of a signatory, etc.

The contract laws of individual states normally imply certain minimum warranties into contracts concerning the quality of the goods and services supplied. The types of quality warranty most commonly imposed include:

- *Objective quality of goods.* The vendor promises that the goods delivered will be objectively satisfactory to a normal purchaser given all of the circumstances of the transaction.[92]
- *Subjective quality of goods.* The vendor promises that the goods delivered will be sufficient to meet the subjective purpose of an individual purchaser, whether or not the goods were originally manufactured for that intended purpose.[93] For this warranty to apply, the purchaser is normally required to disclose the purchaser's specific purpose in advance to the vendor. As a result, this term is rarely discussed in the context of standard online commerce systems, which often do not allow unstructured communication between vendor and purchaser concerning unusual use cases.
- *Objective quality of services.* The service provider promises that it will exercise due care in the process of service delivery.

Upon consideration, a significant distinction emerges between the quality of goods and services warranties. Compliance with the goods warranties is assessed by examining the goods supplied. A warranty that goods will be objectively satisfactory is breached if the goods are poor – without regard to the care taken by the vendor in manufacturing, sourcing, or inspecting goods. By contrast, a warranty that a service provider will take due care is assessed by examining the service provider's actions, qualifications and methodology. It is possible for a service provider to comply with a warranty of due care and yet produce a deliverable which is demonstrably poor or inaccurate. (The basis of this distinction between product and service is becoming increasingly difficult as persons place greater reliance on cloud services as a substitute for products. (See also discussion in Section 7.2.)

Although various laws imply these standard warranties into contracts as a matter of course, it is commonplace – nearly universal – for suppliers of information and communications technologies and services to attempt to exclude these terms by express agreement. Efforts to exclude these baseline warranty protections are viewed with suspicion under the contract laws of various states. As a general proposition, it is more difficult and often impossible to exclude these baseline protections from standard form contracts with consumers. In the context of B2B contracts, however, the rules allowing these exclusions tend to be more liberal.

Information and communications technology vendors normally exclude these baseline implied warranties and replace them with narrowly drawn express warranties concerning the quality of deliverables.[94] The relative utility of these express warranties provided by ICT vendors is questioned with some regularity, especially as regards commercial off-the-shelf software or hardware. It remains an open question to what degree these warranty standards encourage or discourage developer behaviours in addressing security-related aspects of ICT products and services [11].

6.4 Limitations of liability and exclusions of liability

Parties to contracts often use the contract to impose both limitations and exclusions of liability that arise from the contracting relationship. An exclusion of liability refers to a contractual term that seeks to avoid financial responsibility for entire categories of financial loss arising as a result of breach of contract, such as consequential loss, loss of profit, loss of business opportunity, value of wasted management time, etc. A limitation of liability, on the other hand, seeks to limit overall financial liability by reference to a fixed sum or financial formula.

The possibility of imposing and enforcing contractual limitations and exclusions of liability creates a powerful incentive for vendors to establish contractual relationships with customers. The contract be-

comes a risk-mitigation tool. As a result, these exclusions and limitations are ubiquitous in contracts for ICT goods and services.

As with the exclusion of implied warranty terms, limitations and exclusions of liability are viewed with suspicion under most systems of contract law. Once again, limitations and exclusions of liability are most heavily disfavoured when contracting with consumers. Rules allowing these exclusions and limitations tend to be more liberal in B2B arrangements.

There is a wide variation among and between jurisdictions concerning the enforceability of these limitations and exclusions. As a general proposition, civil law jurisdictions disfavour these limitations and exclusions more than common law jurisdictions.

It remains an open question to what degree the relative enforceability of these contractual limitations and exclusions encourages or discourages developer behaviours in addressing security-related aspects of ICT products and services [11].

6.5 Breach of contract

When considering the obligations imposed by contract, it is also important to consider the legal consequences of breaching a contract. A 'breach' of contract is simply a failure to fulfil a promise embodied in the contract. Breaches exist on a spectrum of severity. An individual breach of contract might be considered *de minimis*, moderately serious, very significant, etc.[95] The severity of breach can and often does result in different remedies for the injured party.

In the event of a breach of contract, various remedies provided by courts to non-breaching parties typically fall into the following categories:[96]

- *Damages.* Order the breaching party to pay monetary damages to the non-breaching party that are sufficient to restore the net financial expectation that the harmed party can prove was lost as a result of the breach. This is the most common remedy available. A non-breaching party is often obliged to take steps to mitigate financial harm, and failure to mitigate can serve to reduce an award of damages accordingly.
- *Recision.* Declare that the contract is at an end and excuse the non-breaching party from further performance. This is a more extreme remedy, normally reserved for cases in which the breach is very severe. Alternatively, the terms of the contract might specifically legislate for the remedy of recision under defined circumstances.[97]
- *Specific performance.* Order the breaching party to perform their (non-monetary) promise. This is also considered an extreme remedy. This remedy is often reserved for situations when the breaching party can take a relatively simple action that is highly significant to the non-breaching party (e.g., enforcing a promise to deliver already-written source code or to execute an assignment of ownership of copyright that subsists in a deliverable).
- *Contractually mandated remedies.* The contract itself may specify available remedies, such as service credits or liquidated damages. Courts often treat these remedies with suspicion. The law concerning enforceability of private remedies is complex and varies significantly from jurisdiction to jurisdiction.

The remedies described above are normally cumulative in nature. Thus, a party can both request recision and claim for damages as a result of a breach.

6.6 Effect of contract on non-contracting parties

One potential limitation of the utility of contracts is that enforcement may be limited to the contracting parties alone.

In the context of seeking a remedy for breach, the rule of privity of contract (generally found in common law systems) normally restricts contract enforcement solely to the contacting parties. If Alice and Bob enter into a contract and Alice breaches, under the doctrine of privity Bob is normally the only person who can take legal action against Alice for breach of contract. Charlie, as a non-party, cannot normally take action against Alice for breach of contract even if Charlie has been harmed as a result of the breach. Charlie may, however, be able to take action against Alice under tort law, as discussed in Section 7. In complex supply chains, Bob might be able to assign the benefit of the contract rights (such as warranties) to Charlie. (Even in common law systems, there are circumstances in which parties can expressly vest contract rights in the hands of third parties.)

If Alice is a supplier of services and wishes to limit her potential liability to persons who rely on the outputs of these services, a contractual limitation of liability might not be effective against a non-contracting person like Charlie who relies on her service but is not in privity of contract with Alice. This inability to limit liability to non-contracting parties is a recurring consideration in the development of trust services, in which third parties who rely on trust certificates may have no direct contract relationship with the certificate issuer. (See the discussion at Section 10.)

6.7 Conflict of law – contracts

Deciding which state's law will apply to various aspects of a contract dispute is normally vested within the jurisdiction of the court deciding the dispute. The rules used to decide this question can and do vary from state to state. Within the European Union, these rules have been harmonised for most types of contract – most recently through the mechanism of the 'Rome I' Regulation [105]. Individual US states, by contrast, remain free to adopt their own individual rules used to decide whose law should be applied to aspects of contract disputes. Even with these variations some useful and generalisable principles can be identified.

Express choice by the parties. It is widely accepted that persons who enter into a contract should have some degree of freedom to choose the law that will be used to interpret it. (Rome I, Art 3 [105].) Various policy justifications are available, often built upon notions of freedom of contract. If parties are free to specify the terms of their contractual relationship, this argument suggests that the same parties should be free to incorporate within the agreement anything that assists to interpret the terms that have been agreed – including the substantive system of contract law used to interpret the agreement.

Absence of an express choice of law by the parties. When parties connected to different states do not make an express choice of law in their contract, the court is faced with the dilemma of deciding whose law to apply to various aspects of the contract dispute. In the European Union, rules determining the applicable law in the absence of choice are found in Rome I, Art 4. Of particular interest to those who deal with online contracting systems, are the following default rules in the absence of a clear choice by the parties:

- A contract for the sale of goods or supply of services will be governed by the law of the place where the seller or service provider has its habitual residence. Art 4(a)-(b).
- A contract for the sale of goods by auction shall be governed by the law of the country where the auction takes place, if such a place can be determined. Art 4(g).
- A contract concluded within a multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments in accordance with non-discretionary rules and governed by a single law, shall be governed by that law. Art 4(h).

Thus, we see in European law a baseline policy preference to apply by default the law where the vendor or market maker is resident, over the law where the buyers or bidders may be resident.

Contracts with consumers. When one of the parties to a cross-border contract is a consumer, the rules are generally modified to provide additional protection for the consumer. In disputes in a European Union forum court, for example, if the cross-border vendor of products or services pursues their business activity in the place of the consumer's residence, or 'directs such activities to that country or to several countries including that country', then the following special rules usually apply:

- If there is no express choice of law in the contract, the applicable law will be the law of the consumer's habitual residence. Art 6(1).
- If some other law has been expressly chosen, that choice of law cannot deprive the consumer of legal protections mandated by the law of the consumer's residence. Art 6(2).

Although the specific examples above are drawn from European legislation, they represent principles that regularly occur in other states that face conflict of law issues in consumer contract disputes.

7 Tort

A tort is any civil wrong other than a breach of contract. Unlike contractual liability, tort liability is not necessarily predicated upon a volitional relationship between the person who commits a tort (a 'tortfeasor') and the person harmed by that tortious action (a 'victim').

This section will address a few of the more common tort doctrines that should be considered by cyber security practitioners. Two substantive torts of interest (negligence and product liability) will be examined in some detail together with a series of more general tort doctrines such as causation and apportionment of liability. Rights of action granted to victims under other legal subject matter regimes (e.g., data protection, defamation, intellectual property, etc) are also characterised as tort actions, and the general concepts (see Section 7.3-7.6) often apply to these as well.

7.1 Negligence

Most legal systems recognise the idea that persons in society owe a certain duty to others in the conduct of their activities. If a person fails to fulfil this duty, and the failure causes harm to a victim, the victim is often given a right to take legal action against the tortfeasor for financial compensation.

7.1.1 Duty of care: how far does it extend?

Legal systems implicitly acknowledge that a person is not always responsible to everyone all of the time. Some limitation on the scope of responsibility is normal. The courts of England, for example, have said that one person (Alice) owes a duty of care to another (Bob) in respect of a given activity if three conditions are fulfilled:

1. Alice and Bob are somehow proximate to one another in time and space;
2. it is reasonably foreseeable to Alice that her action (or inaction) could cause harm to persons in a position similar to Bob; and
3. with respect to Alice's action (or inaction), on the whole it seems fair and reasonable for persons like Alice to be responsible to persons in a position similar to Bob.

Although this three-pronged rule is not presented as a multinational norm, it illustrates the general proposition that the scope of civil responsibility owed to others as a result of negligence is limited.[98]

'Foreseeability' of harm is used routinely as a mechanism to limit the scope of liability in negligence law.[99] Foreseeability is normally measured by reference to whether or not an objectively reasonable person would have foreseen harm. A tortfeasor is not excused from liability due to failure of imagination, failure to plan, or an affirmative effort to avoid considering potential victims.[100]

This raises a number of related questions for consideration in the context of cyber security. Examples worthy of further consideration are set out in Table 3.

The purpose of Table 3 is to consider some of the types of relationship that might create a duty of care under existing law.

Negligence laws are tremendously flexible. As harm caused by cyber security failure becomes increasingly foreseeable, it seems likely that courts will increasingly interpret the concept of duty of care to encompass various cyber-security related obligations owed to a broader group of victims [107].

The concept of 'duty of care' does not normally depend on the existence of any business or contract relationship between tortfeasor and victim. As a commonly understood non-security example, automobile drivers are said to owe a duty of care to other drivers, to bicycle riders, to pedestrians, and to others who are expected to use roads and pathways. One might therefore consider the extent to which those who supply software on a non-commercial basis, such as open source security software, might be found to owe a duty of care to those persons who adopt and implement such software.

7.1.2 Breach of duty: measuring reasonableness

If a person (Alice) owes a duty of care to another person (Bob) in the conduct of a given activity, the question arises whether or not Alice has breached (failed to fulfil) her duty to Bob. The formulation of these two elements together – 'breach of a duty of care' – is normally synonymous with 'negligence'.

A typical standard used to assess conduct is to examine whether or not Alice has acted in an objectively reasonable manner. In classic negligence law persons like Alice are not held to a standard of perfection. Liability is based upon fault. In assessing fault, courts often make use of rhetorical devices such as the objectively 'reasonable person' similarly situated.

As a framework for measuring conduct, the reasonable person standard has proven remarkably resilient and flexible over time. Cyber security practitioners often converge with opinions on whether a given cyber security-related action (or inaction) was objectively reasonable or unreasonable. Changes in technology, development of new methods etc. can all serve to revise opinions on the definition of what constitutes 'reasonable' security conduct.

There is a temptation to conflate 'reasonable conduct' with efforts to define so-called 'best practice'. Rapid advances in information technology (e.g., the falling cost of processing capability) routinely alter the cyber security landscape. Disruptive changes in the environment (e.g., the move to the cloud, the emergence of big data, the birth of the Internet of Things) can rapidly de-stabilise received wisdom.

The highly respected US Judge Learned Hand warned of this in two famous decisions from the mid-twentieth Century. Responding to an operator of an ocean-going cargo vessel who argued that the vessel's lack of a working radio did not constitute 'unreasonable' conduct, Judge Hand observed in The T.J. Hooper case in 1932 that 'common practice is not the same as reasonable practice' [108, 109]. Although the vessel operator was following the common practice of his industry in the 1920s, Hand clearly expressed the idea that changes in technology and the environment should spur re-examination of methods and activities.

Fifteen years later in the 1947 *Carroll Towing* case, Hand announced a definition of reasonable conduct that is helpful in assessing whether or not the time has arrived to adopt a new method of operation. His decision set out, in essence, a cost-benefit test [109, 110, 111]. He reasoned that when the burden (cost) of adopting a methodology is less than the mathematical product of (1) the probability of loss in the absence of that method and (2) the amount of the loss to be avoided, then the 'reasonable' action is to adopt that methodology.[102]

The doctrine of 'negligence, *per se*' is sometimes adopted by courts to assess conduct. Using this doctrine, a victim argues that the tortfeasor's conduct should be found to be unreasonable because it

When a potential tortfeasor such as a:	Conducts this activity poorly (in an unreasonable fashion):	Consider whether the potential tortfeasor owes a duty of care to these potential victims:
Retail merchant.	Maintaining security of payment card details supplied by customers at point of sale.	Card holders; Merchant banks; Card issuing banks. [106]
Email service provider.	Managing the security of email servers and related services; Making decisions about the types of security to be adopted.	Service subscribers; Subscribers' third-party email correspondents; Persons named in email correspondence.
Business enterprise.	Managing the cyber security of enterprise IT or OT; Making decisions about the types of security to be adopted.	Its own staff members; [107][101] Its counter-parties and supply chain partners; Unrelated third parties suffering harm when malicious actors compromise the enterprise's security measures and use the enterprise's IT to launch onward attacks; Unrelated third parties who suffer harm when compromised OT causes personal injury or property damage.
Developer of web server software.	Implementing standard cryptographic communication protocols.	Merchants who adopt the web server software for online commerce; SaaS providers who adopt the web server software for the provision of various services to customers; Ecommerce customers who submit payment card details to the server; Business customers who submit sensitive business data to a SaaS provider who adopts the server software; Business enterprises who adopt the server within their IT or OT infrastructure.
Trust service provider.	Registering and confirming the identity to be bound to a certificate; Issuing certificates; Maintaining the trust infrastructure.	Customers who purchase certificates; Third parties who place reliance on these certificates; Third parties who operate equipment which (without their knowledge) places reliance on these certificates.
Web browser developer.	Selects root trust certificates for installation into its web browser.	Persons who use the web browser.

Table 3: Illustration of potential duty of care relationships

violated a public law or widely-adopted technical standard. This doctrine has been pleaded together with standard negligence claims in legal action arising from cyber security-related incidents [106]. This doctrine may become increasingly useful to victims as a result of increasing standardisation and regulation in the field of cyber security.[103] The mere act of defining and adopting security standards can therefore influence courts as they seek technical frames of reference for assessing the 'reasonableness' of conduct.

Another doctrine that may prove useful in analysing cyber security failures is that of '*res ipsa loquitur*' (i.e., 'the thing speaks for itself'). Using this doctrine, a victim who might otherwise have difficulty proving the precise nature of the action that caused harm, claims that the most appropriate inference to be drawn from the surrounding circumstances is that the accused tortfeasor bears the responsibility. This doctrine tends to be used against persons who are supposed to maintain control over risky or dangerous processes that otherwise cause harm. A typical example might include legal action against a surgeon after a surgical instrument is discovered in the body of a post-operative patient, or a wild animal escapes from a zoo. Irrespective of the victim's ability to prove a lapse of caution, the most appropriate inference to be drawn from the circumstances is a lack of due care. (Hence, the thing speaks for itself.) In the field of cyber security, one might imagine a case in which this doctrine is applied in a legal action against a person who creates a new form of malware for research purposes, only to lose containment.[104]

Doctrines similar to negligence *per se* and *res ipsa loquitur* might be defined in some legal systems as rules concerning the reasonability of conduct, or they might be defined as rules of evidence – relieving a victim of some or all of their burden to prove unreasonable conduct, or shifting the burden to the alleged tortfeasor to prove reasonable conduct. (See the discussion of evidence in Section 1.3.)

Although they are not normally considered under the rubric of negligence law, other laws which influence cyber security practice define 'reasonable' conduct within their sphere of competence. An example is found in the law of funds transfer expressed in Article 4A §202(c) of the Uniform Commercial Code as adopted by US states [104].

7.1.3 The interpretation of 'fault' differs by place and changes over time

Although the framework presented above for defining 'fault' is generally well-received by legal systems in most developed economies, this should not be mistaken for agreement on how to interpret or apply these standards.

The interpretation of both 'duty of care' and 'reasonable' behaviour can vary significantly from state to state. This should not be surprising, as both concepts are social constructs anchored by opinions about risk and responsibility that prevail in a given society at a given time.

The interpretation of 'duty of care' has (with some exceptions) mostly expanded over the past century as the increasingly complicated and interconnected nature of modern life creates more opportunity for the actions of one person to harm others. Similarly, the interpretation of 'reasonable' has generally moved in the direction of requiring more care, not less. These interpretations can be expected to change within the working life of a practitioner, especially as the harm caused by cyber security failure becomes increasingly foreseeable, better understood, and easier to prove with new forensic tools.

Similarly, practitioners are cautioned that potentially tortious acts committed in one state might be assessed by the interpretation of standards of care adopted by another, more demanding, state. (See the discussion in Section 7.6.)

7.2 Strict liability for defective products

In the second half of the twentieth Century, a number of states with developed industrial economies adopted rules of strict liability for defective products.[105] This liability regime provides a right of action for those who suffer personal injury, death, or property damage, caused by a defective product. A product is usually deemed to be defective when it fails to provide the safety that a reasonable person would expect under the circumstances. Depending on the specific law in question, strict liability typically attaches to persons who produce, import or sell defective products or component products. Liability can attach without any pre-existing relationship with the victim.

In this type of liability, the focus of analysis shifts away from any notion of 'fault' by the tortfeasor and moves instead to an examination of the allegedly defective product. Liability is generally assessed without regard to the degree of reasonableness used in producing, examining, or selecting products for sale. This type of strict liability is found throughout the laws of the states of the US and is incorporated into EU member states' domestic laws as mandated by Directive 85/374 [112, 113].

Most authorities believe that software, as such, does not fit within the various definitions of 'product' applicable under such laws.[106] Even so, under currently-existing product liability law a defect in a software component can be the source of a defect in a product into which it is installed. Liability of this sort arising from cyber security failures will probably increase as physical control devices are increasingly connected to remote data services, presenting more cyber security-related risks to life and limb.

A cyberspace-connected product (e.g., an autonomous vehicle, an industrial control system, a pacemaker, a vehicle with fly-by-wire capability, a remotely operated home thermostat) that fails to deliver appropriate safety, is defective whether the safety is compromised through failures in electrical, mechanical, software, or security systems. Thus, strict product liability could be implicated in cases of personal injury or property damage whether the safety of the connected device is compromised through errors in operational decision-making (e.g., an autonomous vehicle chooses to swerve into oncoming traffic after misinterpreting road markings) or errors in cyber security (e.g., a flawed or improperly implemented authentication scheme permits a remote hacker to command the same vehicle to divert into oncoming traffic, to open the sluice gates in a dam, or to alter a home thermostat setting to a life-threatening temperature).

In its comprehensive 2018 evaluation of European product liability law, the European Commission referred extensively to the increased role of software and other so-called 'digital products' in modern commerce [114]. The Commission openly questioned the extent to which digital products (e.g., software as a product, SaaS, PaaS, IaaS, data services, etc.) should be redefined as 'products' under product liability law and thus subjected to strict liability analysis when defects cause death, personal injury, or property damage [115]. This is an area of law that could change significantly in the medium-term future.

7.3 Limiting the scope of liability: legal causation

The primary purpose of tort law is to compensate victims for harm suffered. A victim can normally only bring a legal action against a tortfeasor if the victim can prove that the relevant tortious action was the cause of a legally cognisable harm suffered by the victim. Put simply, people may act negligently without liability – if their behaviour causes no harm.

Causation is one of the more difficult concepts to define in law. Different authorities take different views about when it is appropriate to hold a tortfeasor responsible when it is claimed that tortious action A has produced harm B. The victim is often required to prove causation-in-fact as a first step. This concept is also expressed as 'but for' causation, because it can be tested using the logical statement: 'But for tortious action A, harm B would not have occurred.' Liability can sometimes be eliminated by showing that a given harm would have occurred independently of a tortious act

[116, 117].

Causation-in-fact, however, is often not sufficient on its own to prove liability. Difficulties arise when analysing more complex chains of causation where tortious action A causes result X_1, which in turn causes result X_2, ..., which in turn causes result X_n, which in turn causes harm B.[107] As the link becomes increasingly attenuated, policy makers and judges struggle to define the limits of responsibility of the person committing the tortious act. Similar difficulties arise when the 'last cause' in a combination of negligent acts causes harm that is significantly disproportionate to the individual negligent last act, as a result of more serious lapses of judgment by prior actors. Approaches adopted to resolve this issue include limiting the responsibility of the tortfeasor to harm that is reasonably foreseeable [118].[108]

The narrower definition of causation required by tort law may be referred to using terms such as 'legal causation' or 'proximate causation'.

Proving that a specific harm was caused by a specific cyber security incident can be extremely challenging. To take a common example, a natural person whose identification data has been compromised may find it difficult or impossible to prove that the data lost in a given data breach event are the source of the data subsequently used by malicious actors to carry out fraud through impersonation. Data breach notification laws help to redress the imbalance of evidence available to victims in these cases, but even then, the victim must prove a causal link from a specific breach to the fraud event. A notable exception is financial loss incurred following a breach of payment card data, as the causation of subsequent fraud losses can be easily inferred from a contemporaneous data breach event. These cases create other challenges as discussed in Section 7.4.

7.4 Quantum of liability: money damages

Different states have different approaches to defining what constitutes legally cognisable harm for purposes of tort law. A victim is normally required to prove the financial value of harm caused by a tortious act.

In cases involving personal injury, the value of the harm is often calculated by reference to easily understood measures such as: loss of salary suffered by the victim due to their inability to work, costs incurred by the victim for medical treatment, rehabilitation, or nursing care, costs of installing accommodation facilitates for a permanently injured victim, etc. Some states also allow compensation for harm in personal injury cases that is more difficult to quantify such as pain and suffering, emotional distress, etc.

A recurring issue in negligence cases concerns whether or not a victim can recover for so-called pure economic loss. There is a divergence in the law on this question. A leading case in England concerned the economic loss caused by a poorly considered credit reference provided by a bank to its customer. Although the loss (the customer's subsequent inability to collect a trade debt from its insolvent client) was purely economic in nature, the English court decided it should be recoverable because the bank professed special skill (financial awareness), and the victim relied on the flawed statement to its detriment [119].[109]

A growing number of cases have been brought on the basis of negligent cyber security which claim losses other than personal injury or property damage. Some courts have already exhibited a willingness to award damages under the law of negligence to victims whose losses are purely economic in nature [107].[110] Other legal actions (settled by the parties before trial) have involved substantial claims for economic losses based on negligent cyber security.[111]

Proving legally cognisable harm can be challenging for some victims who might otherwise wish to take legal action based on cyber security failures. One example concerns the loss of privacy. There is a lot of argument about how to quantify (financially) the harm caused by breach of privacy unless the victim has some business or economic interest that is directly harmed as a result.[112]

Another common example concerns the loss of confidentiality of financial authentication methods such as payment card details. Card holders would have difficulty proving harm to the extent that fraudulent charges are refunded by the issuing bank. Of course, the issuing bank will then be able to demonstrate financial harm as a result of refunding these monies, plus a *pro rata* portion of the costs incurred issuing replacement cards earlier than planned.

In response to these types of difficulties in proving harm, some states have adopted specific laws that provide a schedule of damages that can be claimed without the need to quantify harm. An example is found in the State of Illinois Biometric Information Privacy Act, which provides that any party aggrieved by a violation of the act can take legal action and recover US$1,000 per violation (for negligent violations) or US$5,000 per violation (for intentional violations) of the law's mandates.[113] Similarly, US copyright law allows some rights owners to recover minimum damages using a statutory tariff.

Some jurisdictions, notably member states of the United States, are prepared to award 'punitive damages' in some tort cases. These awards are intended to punish and deter bad behaviour. These awards can be disproportionate compared to the underlying award for the harm suffered by the victim. Examples where a court might award punitive damages most commonly include cases where the tortfeasor demonstrates a pattern of repeated poor behaviour, or the tortfeasor has made relevant operational decisions with gross indifference to human life or human suffering.

7.5 Attributing, apportioning and reducing tort liability

This section discusses a few miscellaneous legal doctrines that are important to consider when attempting to assess risks of tort liability.

7.5.1 Vicarious liability

There are circumstances when the liability of a tortfeasor can be attributed to a second person. The situation commonly encountered in cyber security is liability for the tortious act of an employee attributed to their employer. This type of vicarious liability applies when the tort is committed during the course of an employment relationship.

Vicarious liability is strict liability. Once a victim proves that the employee committed a tort which caused relevant harm and then proves that the tort was committed within the course of employment, the employer becomes strictly liable for that underlying tort. Pleas by the employer about taking reasonable precautions, mandating reasonable training, due diligence when hiring or the employee's deviation from employment standards, are generally ineffective against claims of vicarious liability.

The Court of Appeal in England in 2018 affirmed a vicarious liability claim brought in a data protection tort action. In *Wm Morrison Supermarkets PLC vs Various Claimants*, the data controller Morrison was sued by various data subjects after a disgruntled internal audit employee published salary data of 100,000 employees in violation of data protection law.[114] The secure handling of salary data fell within the field of operation with which the employee was entrusted and therefore the tort was committed by the employee within the scope of the employment relationship, thus leading to vicarious liability [88]. At time of writing, this decision is pending appeal in The Supreme Court of the United Kingdom.[115]

The only reliable method to avoid vicarious liability is to encourage employee behaviour that limits or avoids tortious activity. This is worthy of consideration by those who develop and enforce acceptable use policies, staff security standards, employment policies, etc.

7.5.2 Joint and several liability

In cases where more than one tortfeasor can be said to have caused harm to a single victim, tort law often allows joint and several liability. The doctrine is simple: any jointly responsible tortfeasor might be required to pay 100% of the damages awarded to a victim if the victim is unable to collect from

the other tortfeasors. Although the tortfeasor satisfying the victim's financial claim may have the right to pursue compensation (a.k.a. 'contribution') from other tortfeasors, this becomes problematic when the joint tortfeasors have no financial resources or are resident in foreign states where there is no effective method of enforcing such rights.

Persons may wish to consider the impact of this rule when working with supply chain partners or joint venturers who are small, who do not have much capital, or who are resident in a foreign state where enforcement of domestic judgments would be problematic.

7.5.3 Affirmative defences

Tortfeasors are sometimes able to take advantage of certain affirmative defences to tort claims. A tortfeasor who is able to prove the relevant elements of these defences can reduce, or sometimes eliminate, their liability.

In the context of negligence, a common category of defences includes 'contributory negligence' or 'comparative fault' of the victim. In this type of defence, the tortfeasor attempts to prove that the victim's own negligence contributed to their harm. Depending on which state's tort law is applicable to the claim, a successful defence can reduce or eliminate liability to the victim.

Another category of defence that can be useful in various cyber security contexts include 'assumption of risk' or 'consent'. In this type of defence, the tortfeasor avoids liability by proving that the victim was aware of, or knowingly consented to, the risks that ultimately caused the harm. This type of defence can be especially useful for those who supply cyber security services that risk damage to client infrastructure, such as penetration testing. Practitioners often draft commercial engagement documents with a view to attempting to satisfy one of these defences in the event that something goes wrong during the engagement.

As regards strict product liability, many states offer a so-called 'state of the art' defence. Where this defence is allowed, a party can avoid strict liability by proving that a product, although defective, was produced at a time when the technological state of the art would not have enabled discovery of the defect. It is debatable how this defence might apply to products made defective as a result of cyber security flaws.[116] Of greater significance, perhaps, is the affirmative defence against strict liability for a defective product available if the defending party can prove that the defect is present due to compliance with laws or regulations concerning product design.[117]

7.6 Conflict of law – torts

Deciding which state's law applies to various aspects of a tort dispute is normally vested within the juridical jurisdiction of the forum court deciding the dispute. The rules that are used to decide this question can and do vary from state to state. Within the European Union, these rules have been harmonised for most torts through the mechanism of the 'Rome II' Regulation [120]. Individual US states, by contrast, remain free to adopt their own individual choice of law principles when deciding whose law should be applied to aspects of tort disputes. Even with these variations some useful and generalisable principles can be identified.

Broadly speaking, courts who examine tort claims between parties in different states tend to settle on two methods to decide whose law to apply: adopt the law of the place where the tortious act originated or adopt the law of the place where the injury was suffered. Historically, it might have been difficult to find cases where these two events occurred in different states. Modern commerce, however, has produced a number of cases where the two events can be widely separated by space and time.[118]

In disputes heard in courts throughout the European Union, the applicable law in a tort action (with some exceptions) is the law of the place where the damage was suffered. (Rome II, Art 4(1).) In cases of product liability, the rules are slightly more complex and the applicable law might be the

place of the injured party's habitual residence, the place where the product was acquired, or the place where the damage occurred. (Rome II, Art 5.)

The above rules provide a reasonable indicator of the risk that cyber security failures occurring due to actions performed in State A, and subsequently causing harm to persons in State B, could easily become amenable to liability analysis under the tort law of State B. Thus practitioners (and their employers) might be held to a higher standard of care imposed by a foreign state where victims of negligent cyber security or defective IoT products are found.

8 Intellectual property

[12, 13]

The complexity of intellectual property law prompted a nineteenth-century US jurist to comment that this subject is closest to 'the metaphysics of law'.[119] Metaphysical or not, intellectual property can serve to constrain or encourage actions by cyber security practitioners. This section will summarise some points where the two fields intersect.

8.1 Understanding intellectual property

Intellectual property rights are negative rights – they convey the right to demand that other persons cease a prohibited activity. The nature of the activity to be prohibited is defined in the law establishing that right. Ownership of intellectual property normally conveys the right to take legal action against others demanding that they both cease prohibited acts and pay money damages arising from infringement.

Intellectual property rights do not give the affirmative right for the owner to take any action imaginable with the subject matter. A given action (combining one's own code with others, abusive IP licensing practices) could infringe third-party intellectual property rights or trigger liability under competition law, among others.

Registered intellectual property rights (e.g., patents and registered trademarks) are granted on a state-by-state basis following application to an appropriate state agency, often following examination by state officials. Unregistered intellectual property rights (e.g., copyright) usually spring into existence without any need for intervention by state officials.[120]

The term 'public domain' can cause confusion. In the field of intellectual property law, 'public domain' refers to a work in which no current intellectual property right subsists. By contrast, the phrase 'public domain' is also used colloquially to indicate a lack (or loss) of confidentiality. To distinguish these two, if a confidential original written work is subsequently published the contents become publicly known. Confidentiality has been lost. This work, however, may still be protected by copyright unless these rights are expressly relinquished. In contrast, if a person who writes software then declares that they are placing the code in the public domain this statement is often treated as an irretrievable relinquishment of copyright. The term should be used with care.

8.2 Catalogue of IP rights

This section will describe some of the IP rights most likely to be encountered by cyber security practitioners. Additional IP rights that may be of interest to practitioners, but which are not addressed in this section, include protections for semiconductor topographies, the EU *sui generis* right to prevent the extraction or reutilisation of the contents of a database, and registered and unregistered design rights.

In many circumstances, contract rights (especially licensing agreements) supplement intellectual property rights and may be treated informally as a type of intellectual property. To make matters more confusing, persons in business often use the phrase 'intellectual property' in an expansive

and colloquial fashion to refer to any work product or process that is the result of intellectual effort - whether or not it incorporates legally recognised and enforceable intellectual property rights. This section deals only with legal rights, as such.

8.2.1 Copyright

Copyright[121] is an unregistered right that springs into existence on the creation of a sufficiently original work. Copyright subject matter includes literary works, which for this purpose includes software code (both source and executable code). This makes copyright especially important for the developers and users of security products embodied in software.

The scope of copyright is generally said to be limited to the expression of an idea rather than the idea itself. Thus, copyright in software code normally protects only the code as written and not the functionality of the resulting software product. Protection of functionality is usually the province of patent law.

The term of copyright is, by ICT standards, extremely long. Literary works are normally protected for the life of the author plus 70 years following their death. While the term of copyright protection granted to computer software may be less than this, it remains sufficiently long that the expiration of the copyright term is unlikely to apply to any relevant software encountered by a security practitioner within their lifetime.

Infringement of copyright normally consists of acts such as copying, transmitting, displaying or translating a significant part of the protected work. Proving that one work infringes the copyright embodied in a second work requires proof of copying. Copying can be inferred from sufficient points of similarity between the two works – there is no need to prove knowledge of copying by the accused. A plethora of forensic techniques have been developed over the course of decades to assess infringement of software source code.

Liability for copyright infringement can sometimes be avoided through various 'fair use' or 'fair dealing' limitations. These are defined differently from state to state.[122]

The scope of copyright protection was expanded at the turn of the twenty-first century to encompass the right to take legal action against persons who interfere with the technological measures used to protect copyright works [121] at Art 11.[123] This was intended to provide additional legal rights of action against those who circumvent technologies such as digital rights management systems (see the discussion in Section 8.4.) [122].

8.2.2 Patents

A patent is a registered intellectual property right, granted on a state-by-state[124] basis following application and examination. Patents are meant to protect an invention that is novel and that also includes an additional distinguishing characteristic variously described by states as an 'inventive step', a 'non-obvious' character, or something similar. This inventive step requirement is a policy device used to limit patent protection to inventions that are significant in some fashion, rather than trivial.[125] Novel inventions that would have been obvious to a person skilled in the relevant technical art are normally denied patent protection.

States expressly define additional subject matter that may not be claimed as a patented invention. Common exclusions of special interest to security practitioners are software, *as such*, and an idea or mathematical formula, *as such*.[126] Inventions that embody these, however, can be patentable subject matter in appropriate circumstances.

The US patent system has changed its approach to software patents in the past few decades and is increasingly receptive to them. Even states that notionally reject the concept of software patents regularly grant patents on inventions that are embodied in software. In other words, software patents (crudely speaking) are a regular feature of the ICT domain.

Cyber security-related inventions that appear on their face to be purely mathematical or algorithmic (e.g., cryptographic methods) can be the subject of patent protection as embodied in various devices – including software-enabled devices. Aspects of historically significant cryptography inventions have been protected by patents, including DES, Diffie-Helman, and RSA [123]. Although the patents on these breakthrough cryptographic inventions have now expired, the field of cyber security innovation remains awash with patents and pending patent applications [124, 125, 126].

The price of a patent is paid in two forms: money and public disclosure. Applications are expensive to prosecute and expensive to maintain. The process of navigating international application and examination is sufficiently complex that (expensive) expert assistance is always advisable, and often critical to success. In addition to application and examination fees paid to states, those who are granted a patent are then required to pay period fees to maintain the patent throughout its life.

Beyond the monetary cost, public disclosure is a core feature of the patent system. The patent application must disclose how the invention works in a manner that would enable a skilled technical practitioner to replicate it. The application and the granted patent, together with examination correspondence,[127] is normally published to enable future study.[128]

The term of a patent is normally 20 years from the date of application. Patents are typically subjected to an examination process which can take years to conclude. When a patent is granted, the right holder is normally given the right to take legal action retrospectively for infringements that took place after the application but before the grant, even if the infringement happened prior to the publication of the application.[129] The validity of a patent can be challenged post-grant as a method of defending against legal actions taken by the right holder.

Infringement of a patent normally consists of acts such as manufacturing, distributing, importing, exporting or selling a product or service that embodies the claimed invention. Proving infringement involves a forensic comparison of the accused device or service with the invention as claimed in the granted patent. There is no need for a right holder to prove that the invention was copied from the patent or from any product. Many people who infringe ICT-related patents do so initially without any awareness of third-party products or patent rights.[130]

8.2.3 Trademarks

Trademarks are usually registered[131] intellectual property rights, granted on a state-by-state basis following application.[132]

A trademark is a symbol or sign used to distinguish one person's business or products from another's. The most common trademarks consist either of words or figures.[133] Trademarks are granted within defined use categories, meaning that it is possible for two different persons to have exclusive rights for the use of the same symbol in different lines of business. The purpose of trademarks is to reduce the possibility of confusion for those who procure goods or services, and to protect investment in the reputation of the enterprise supplying those goods or services.

Trademarks are normally registered for a period of 10 years, although these registrations can be renewed indefinitely.[134]

Infringement of a registered trademark normally consists of displaying an identical or confusingly similar mark in combination with products or services that fall within the registered scope of exclusivity.[135] Proving infringement involves comparing the accused sign with the registered trademark and assessing whether the two are identical or confusingly similar. There is no requirement to prove that the accused party has actual knowledge of the registered trademark.[136]

Infringement of trademark can occur through the use of a domain name identical or confusingly similar to a registered mark. This creates well-known tensions, as domain names are (by definition) globally unique, while trademarks are not. To prove that the use of a domain name constitutes infringement of a registered trademark, a rights owners must normally prove that the domain name is identical or

confusingly similar to the mark, and that the domain name is used in the supply of goods or services within the scope of exclusive use defined in the trademark registration.

Certification marks are a type of trademark that is used to demonstrate conformity with a given standard.[137] These marks are registered by a standards body, which then grants licences to use the mark subject to compliance with the relevant standard. Any person who supplies relevant goods or services bearing the mark that does not conform with the relevant standard risks legal action for trademark infringement.

A collective mark is a trademark that is used to identify the members of an association, such as a professional society. Having registered the relevant collective mark, the society can take action against those who use it without authorisation, and revoke authorisation from those whose membership has ceased.

8.2.4 Trade secrets

Trade secrets were traditionally protected under general tort law, giving persons who attempted to keep their secrets the right to take legal action against those who inappropriately obtained, used or disclosed these secrets. As the twentieth century progressed, a trend emerged to increase the legal protection of trade secrets. The position of individual US states has been significantly harmonised since the 1980s, and the US federal government adopted the Economic Espionage Act 1996 as a national trade secret law to deter trade secret theft [127, 128]. The European Union significantly harmonised its approach to trade secrets with effect from 2018 [129].

The subject matter of a trade secret is generally regarded as information that is secret, is valuable because it is secret and remains secret due to the reasonable efforts of the secret keeper. Subject matter can include information as diverse as an ingredients list, a method of manufacture, a customer list, an algorithm or details of a patentable invention prior to patent application and publication. Examples of current trade secrets in ICT include the finer details of Google's PageRank algorithm and various proprietary cryptographic algorithms.

Maintaining confidentiality is a core element of protecting a trade secret. Trade secrets can be protected indefinitely so long as secrecy is maintained.[138] Unfortunately, loss of trade secrets through acts of cyber industrial espionage are believed to be widespread and should be a source of major concern for cyber security practitioners [130]. Loss of confidentiality of patentable subject matter can be especially damaging, as publication of inventive details by a third party prior to patent application normally destroys patentability (as the invention then ceases to be 'novel').

Owners of trade secret rights can normally take legal action against persons who misappropriate their secrets. In some circumstances, owners of a trade secret can also take legal action against third parties who receive a trade secret from a mis-appropriator (see the discussion in Section 8.4.2).

8.3 Enforcement – remedies

8.3.1 Criminal liability

In certain egregious circumstances, infringement of intellectual property – especially copyright and trademark – can be prosecuted as a crime. These prosecutions usually require proof that the infringing party was aware of the infringement and are often based on a pattern or practice of infringing these rights, *en masse*.

Those who violate legal prohibitions against anti-circumvention technologies for commercial advantage or financial gain, face a maximum sentence under US copyright law of 5 years for a first offence and 10 years for a second offence.[139] Under British copyright law a person who manufactures, imports, distributes, etc., a device intended to circumvent these protections faces a maximum sentence of 2 years.[140]

Some states classify the knowing misappropriation of a trade secret as a crime. The US adopted a national trade secret criminal law in 1996 [128]. These laws can serve as a basis (not necessarily the only one) for the criminal prosecution of industrial espionage activity.

Some states do not define misappropriation of trade secrets as a crime.[141]

8.3.2 Civil liability

A rights owner is normally able to take legal action against a person for infringement of intellectual property. Remedies for infringement normally include monetary damages, which may be calculated by reference to a so-called reasonable royalty, a statutory tariff or a demand that the infringer make an account of any profits – a demand to pay to the rights owner the economic benefit gained from the infringement.

Civil remedies may also include orders to seize, and perhaps destroy, products that infringe intellectual property rights. These orders are especially useful when interdicting shipments of 'knock-off' goods that embody trademark or copyright infringements.

With respect to trade secrets, persons in the US who suffered misappropriation of a trade secret traditionally brought legal action under the relevant law of their individual state. In 2016, the US national government adopted the 'Defend Trade Secrets Act 2016' amending the Economic Espionage Act to authorise private rights of action under federal law for the misappropriation of trade secrets [131].

A common civil remedy for the infringement of intellectual property is a court order addressed to the relevant infringing party to cease any ongoing infringing activity. In the context of patent enforcement, this can be especially devastating, as an enterprise finds itself unable to continue manufacturing or selling an infringing product. In the context of trade secret misappropriation, this might include an order to cease manufacturing products employing the trade secret or an order prohibiting the publication of the trade secret.

In an online context, such orders might demand that content suppliers or server hosts take down content that infringes copyright or a trademark. Parties who enforce patents have sought orders to force a service provider to stop the operation of infringing services delivered via an online environment [132].

8.4 Reverse engineering

Reverse engineering, 'the process of extracting know-how or knowledge from a human made artefact', has generally been recognised as an accepted practice although treated differently within various categories of intellectual property law [133, 134]. Reverse engineering has historically been viewed as the flip-side of trade secret misappropriation. While trade secret law prohibits the misappropriation of a trade secret (e.g., industrial espionage, bribery etc.), the scientific study of a device sold and purchased in a public sale in an effort to learn its secrets has generally been viewed as 'fair game'. If a trade secret is successfully reverse engineered in this fashion and published, it ceases to be a trade secret.

Since the turn of the twenty-first century, however, the legal treatment of reverse engineering seems to have shifted following the adoption of laws prohibiting interference with anticircumvention technologies, generally making these activities more difficult [135, 136].

Most difficulties arise in the context of reverse engineering software products. Software licenses often contain onerous restrictions, including some limitations on reverse engineering generally and/or reverse compiling specifically. European law generally prohibits any restriction on the ability of an authorised software user to observe and study the functioning of this software, and also grants these users the limited right to reverse compile specifically for the purpose of gaining interoperability information [137].

Pamela Samuelson has produced a useful comparative summary of this confusing landscape [138].

8.4.1 Circumventing copyright technological protection measures

Following the expansion of copyright law to prohibit the circumvention of technological protection measures, those who wish to meddle with these measures do so at their peril. The implementation of these laws provides some exceptions to liability for research in specified circumstances, although the precise circumstances vary. Each exception relied upon must be examined with care.

British copyright law, for example, includes a specific exemption to liability for circumventing protection measures in copyright works *other than a computer program*, for persons conducting research into cryptography, 'unless in so doing, or in issuing information derived from that research, he affects prejudicially the rights of the copyright owner' (CPDA s.296ZA(2)). In other words, one of these researchers might face peril under the law if they were to publish details that made it possible for others to circumvent the protection measures. There is no such general exception in British law for cryptography research involving the circumvention of measures on computer programs (CPDA s.296).

8.4.2 Testing a proprietary cryptographic algorithm

Security researchers hoping to test the strength of a cryptographic system normally require access to the relevant algorithm. This arises naturally from Kerckhoffs's Principle and is well-known to cryptographers. A person who wishes to test the security capabilities of an algorithm encounters practical difficulties when the manufacturer of the product employs a proprietary algorithm protected by trade secret and does not wish to disclose it for testing.

In the *Megamos Crypto* case *(Volkswagen v Garcia)*, the cryptographic product under examination (a special purpose processor chip used in automobile engine immobilisers and keys) was manufactured under license by the algorithm's developer. The testers (academic researchers) did not reverse engineer this product, which could have been accomplished using an expensive chip slicing technique. They chose instead to recover the algorithm by reverse engineering software written by a third party (Tango Programmer) who implemented the Megamos algorithm [139].

They intended to publish the results of their analysis, which would have disclosed the algorithm. Parties who had an interest in the trade secret status of the algorithm brought legal action in the English courts to halt publication. The English High Court was confronted with a request to prohibit publication of the research pending a full trial on the merits. The court seemed to accept that if the researchers had recovered the algorithm from the product itself using the chip slicing technique, there would be no case to answer. But the court found that there was a possibility that the third-party Tango Programmer software may have existed only as a result of trade secret misappropriation, and that the researchers should have been aware of this. The court issued a preliminary injunction prohibiting publication [140, 141]. The case was settled before trial commenced, and the researchers eventually published a version of their paper having redacted a component of the algorithm [142].

8.5 International treatment and conflict of law

The existence of intellectual property rights and assessment of first ownership are normally measured by reference to the place where these rights come into existence [120].

After creation in one state, the existence of copyright is generally recognised in most states around the world by the operation of various copyright treaties [143]. If an author writes some software while resident in State A, the copyright laws of State A are normally viewed as the source of authority for identifying the existence and first ownership of that copyright, while treaties oblige most other states to enforce that copyright within their territories (subject to limitations or exclusions granted by those states).

Grants of registered intellectual property rights (e.g., patents and registered trademarks) are made on a state-by-state basis. When identical or confusingly similar trademarks are registered in different states to different owners, the rights of each owner are equally valid within their respective registered territory. This can cause confusion when a trademark owner in one state makes an accusation of infringement against the owner of a second, nearly identical, trademark in another state [144].

IP rights infringement, and defences to infringement, are normally assessed by reference to the law of the place where the intellectual property is infringed [120]. In cases of copyright, the courts show a persistent willingness to apply the rules (and limitations) imposed by their domestic copyright laws with respect to works that are distributed or displayed in-state via the Internet [1, 33]. The courts are also willing to enforce domestic patents against domestic instantiations of claimed inventions delivered as part of a global service offering [132].

9 Internet intermediaries - shields from liability and take-down procedures

[12, 13]

During the 1990s, policy makers around the world adopted special exceptions to shield certain communication service providers from liability for online content in prescribed circumstances. The changes were made in response to early cases that held these communication service providers liable under then-existing interpretations of content liability laws including copyright and defamation.

In the European Union, these exceptions to liability were generally mandated by Articles 12-15 of the Ecommerce Directive. These provide generalised liability shields in respect of 'mere conduit', 'hosting' and 'caching' services [101].[142] These principles are transposed into member state law in the usual fashion.

In US law, various shields from liability arising under copyright, defamation etc., have been adopted on a subject-by-subject basis.[143]

The widest scope of exemption from liability is normally afforded to those whose service consists of acting as a mere conduit for data.[144] These carriers are often exempted from liability without exception, although they may be ordered to filter traffic as part of a court-ordered enforcement plan [33].

Those who provide a service that consists of nothing more than hosting data are often exempted from content-related liability, unless and until they have reason to know that their infrastructure is hosting illicit content.[145] At this point, they often have an obligation to take down offending content 'expeditiously'. Confusion over how to implement this obligation resulted in changes to some laws which now specify in detail how take-down notices should be sent to hosting organisation, and how hosting organisations are required to reply to these notices.[146]

The topic of shielding service intermediaries from liability is not without controversy. Policy makers re-examine these liability exception provisions from time to time [145, 146, 147]. In 2018, the US Congress amended the main US content liability shield so that it no longer protects any person in cases arising from claims of promoting prostitution or acting in reckless disregard of sex trafficking.[147]

10 Dematerialisation of documents and electronic trust services

As the age of ecommerce slowly developed, lawyers and technologists began to confront the general problem of how the law would treat the process of engaging in relationships using remote electronic media. Three categories of legal issues emerged. The first concerns the admissibility of electronic documents into evidence in legal proceedings. The second concerns various problems of form when transitioning to electronic documents. The third concerns the difficulty of analysing and rationalising rights and responsibilities in the provision of identification trust services – often delivered using electronic certificates.

10.1 Admission into evidence of electronic documents

The admissibility of electronic data as evidence into legal proceedings, once the subject of much suspicion by courts and tribunals, has now become commonplace. Policy makers and judges have become increasingly confident as practitioners have developed forensic techniques to assure the authenticity and integrity of this data. Occasionally, local rules mandate special procedures for admitting electronic evidence. While forensic disputes about the weight to be accorded to this evidence persist, this is conceptually no different from arguments that might arise about any other type of recorded evidence.

10.2 Requirements of form in general

A requirement of form is any obligation imposed by applicable law that a given communication will be given legal effect if and only if it takes a prescribed form. Different states have adopted differing requirements of form over the course of centuries in response to whatever policy issue was ascendant at the time. As a result, these requirements are remarkably diverse and can arise in a wide variety of circumstances.

Examples of requirements of form adopted by various states include rules demanding that, in order to be enforceable:

- certain legal notices must be delivered in writing;
- certain types of promise must be in writing and 'signed' by (or 'executed under the hand of', etc.) the party against whom enforcement is sought;
- certain submissions to a regulatory agency or court must be made using a specified form;
- certain contract clauses or notices that seek to restrict liability must be presented in a prominent fashion (e.g., all in uppercase letters, bold or italic font, etc) to the party against whom they are to be enforced;
- certain contract clauses that seek to restrict liability must be initialled by the party against whom they are to be enforced;
- a last will and testament must be delivered in writing and signed by the testator in the presence of a prescribed number of witnesses, who must also sign the document;
- a document transferring title to certain types of property must be signed in the presence of a state judicial official, who must then affix an official seal to the document.

Electronic trading systems developed as early as the 1960s (see Section 6.2.2) managed to work around many such problems. These systems were typically restricted to subject matter that creates relatively few problems of form or that can be overcome using a framework contract. Participants enter into written agreements (with wet-ink-on-paper signatures or following whatever other requirement of form might be imposed on these contracts), and these constitute the foundation of the contractual relationships between participants.

Newer trading platforms built on open standards, often directed to both businesses and consumers, made early gains by trading in subject matter (e.g., the sale of books and other small consumer goods) where contracts could be concluded, and payments settled, with few if any challenges based on requirements of form.[148]

There is a broad international consensus that it should be possible to create and conduct business relationships in an online environment. In 1996, the United Nations formally encouraged all states to enable online trading relationships [148]. Many states around the world contemporaneously adopted

a variety of laws and regulations designed to enable the online conduct of various types of transactions, trading relationships, administrative reporting, court filings, etc. Many were adopted in the specific context of enabling digital signatures and trust services, as discussed in Section 10.3.

The legal enforceablity of communications related to other subject matter, especially topics such as the disposition of a deceased's estate and the transfer of title to immovable property, have been slower to transition to electronic platforms. These often retain significant requirements of form that make the electronic implementation of relevant communications impracticable unless and until states decide to amend their laws.

10.3 Electronic signatures and identity trust services

The emergence of modern ecommerce was contemporaneous with the emergence of identity trust services, specifically those that issue digital certificates in a public key infrastructure that bind the identity of a person with a given public key.

As engineering standards for these identity trust services began to emerge, two related legal questions surfaced for consideration by anyone who wished to provide or make use of these services:

- the extent to which a digital 'signature' produced using such a system would be accorded legal equivalence with a wet-ink-on-paper signature; and
- the nature of rights and responsibilities of various persons involved in the maintenance and use of these systems.

The question of legal equivalence for signatures is merely a sub-set of the more general problem of requirements of form discussed in Section 10.2. To the extent that various laws impose a requirement to 'sign' a communication, many states have adopted laws to provide legal equivalent to electronic signatures in most, but not all, circumstances.

The question of rights and responsibilities of persons involved in trust service arrangements is significantly more complex [149].

Consider first the potential liabilities of a certificate issuer in a standard three-corner operational model.[149] The law of negligence (see Section 7.1) immediately creates a number of challenges for any person operating as a certificate issuer, among them: what is the nature of the duty owed to a third party relying on a certificate; what are appropriate standards of care in this new operational model; and what harm is foreseeable when errors occur? Specific liability scenarios range from a system-wide disaster caused by the undetected compromise of a root certificate or technical flaw in the authentication mechanism, to the occasional (although recurring and perhaps inevitable) cases of improperly issuing a certificate following the misidentification of a signatory.

Consider also the potential liabilities of a signatory or a third party who relies on a certificate. Early policy debate focussed significantly on the degree to which signatures should be binding on the relevant signatory – especially when that person may have lost control of the signature creation device. This is a surprisingly old issue in law, commonly encountered in the context of cheque-signing machines, signature stamps, and the like, adopted by businesses, financial institutions, medical professionals, etc. Much of the policy debate over this issue appears now to be concentrated on the subject-matter laws governing specific use cases, such as those adopted to regulate electronic payment services [103, 104].

A lack of certainty over these issues has caused certificate issuers to seek out methods to limit or otherwise rationalise their liability. A common strategy for limiting liability, entering into contracts which include limitation clauses, faces a significant problem. Forming a contract between the issuer and the relying person normally requires the communication of offer and acceptance between these persons

(see Section 6). Most systems were designed to enable reliance without the constant intervention of presenting a user with new terms and conditions every time a relying party encountered a new certificate vendor. Similarly, certificate issuers might wish to warn relying parties about the scope of appropriate subject matter for which the certificates might be used.

The technology development community attempted to address these concerns by incorporating in the certificates specific data fields designed to communicate reliance limits and scope of use limits.[150] This strategy faced a different set of legal challenges. In practice, the certificates tend to be buried in rarely-accessed segments of the user interface. Further, a vast number of end users whose machines might be relying on these certificates would likely fail to comprehend the data presented in them, as certificate data tends to be presented in a highly technical fashion. In these circumstances, significant doubt has emerged about the ability to create an enforceable limitation of liability between the certificate issuer and the relying third party.[151]

States and legal experts intervened with a variety of recommendations, and then laws, attempting to address these issues [150, 151, 152, 153].[152] These laws, often identified with the term 'digital signature' or 'electronic signature' in their titles, typically adopted a combination of the following policy interventions:

- mandating the acceptance of electronic signatures as legal evidence;
- mandating the legal equivalence of electronic signatures that meet certain minimum technical characteristics to assure message authentication and integrity;
- instructing judges that electronic signatures (even those which provide little or no technical assurance of authentication or integrity) cannot be refused legal equivalence merely because they take an electronic form, but leaving open the possibility of denying equivalence for other reasons;
- imposing on a certificate issuer a duty of care owed to third parties who rely on certificates;
- establishing frameworks for regulation to encourage higher technical and non-technical standards of care in the operation of a certificate issuance business;
- allowing certificate issuers to limit their liability by reference to a financial sum presented in the certificate itself, whether or not the relying third party actually reviews this limitation; and
- allowing certificate issuers to exclude liability by reference to a subject matter limitation presented in the certificate itself, whether or not the third party actually reviews this exclusion.

There is some degree of variance between states on how they have chosen to address these issues. A recurring theme concerns the unwillingness of law makers to reduce rights otherwise afforded by consumer protection laws.

While some of these laws are general in nature, others are more narrowly drawn to address specific subject matter. In some cases, the law delegates authority to a regulatory body to adopt specific secondary legislation and/or technical standards on a subject-specific basis. Any practitioner who hopes to develop a platform in an area where requirements of form are commonplace must research and review applicable laws and regulations to reduce enforceability risk.

While much debate and discussion has focused on certificate issuers, signatories and third parties who rely on certificates, another actor in this domain is more often overlooked: the person who selects which certificate issuers should be trusted by default. This 'certificate issuer selection' role is routinely undertaken, for example, by producers of consumer web browsers. This is perhaps inevitable, as the vast majority of end users would have no rational method of discriminating between good-quality and poor-quality certificate issuers. This raises the question of defining what duty of care these certificate issuer selectors might owe to end users.[153]

10.4 Conflict of law – electronic signatures and trust services

The nature of electronic signatures and trust services invariably implicates conflicts of law when relevant parties are in different states. Consider a certificate issuer located in State A, a signatory located in State B who procures a certificate and uses it to create digital signatures, and a third party relying on the certificate located in State C.

Assessing the legal equivalence of the signature can become complicated depending on which law imposes a relevant requirement of form that mandates a 'signature'. In the case of documents that purport to transfer title to immovable property, the legal equivalence question will almost certainly be answered by reference to the law of the state where the immovable property is located. The state where the immovable property is located is, in nearly all circumstances, the only one that can credibly assert enforcement jurisdiction over a title dispute as it is the only sovereign that could seize the property. In matters of a simple contract between a non-consumer signatory and non-consumer third party, the European courts should be willing to find formal validity of the contract if it meets the requirements of validity applied by the law of the state chosen by the parties to govern the contract, the law of State B, the law of State C, or possibly the law of either party's habitual residence if different from any of these (Rome I, Art 11) [105]. Where consumers are involved, the European courts would only find such a cross-border contract valid if it was deemed valid under the law of the consumer's habitual residence.

Determining the applicable law concerning limitations of liability is similarly complex. Consider, for example, the ability of a certificate issuer to rely on a limitation of liability granted under the trust services or digital signature law of State A. If the third party in State C brings a negligence action against the certificate issuer, the applicable tort law may well be the law of State C – which would not necessarily recognise the liability limitation granted by State A law, especially in cases where injured persons are acting as consumers.

11 Other regulatory matters

This section will briefly address additional miscellaneous regulatory topics that a cyber security practitioner might be expected to encounter.

11.1 Restrictions on exporting security technologies

States have long imposed restrictions on the export of goods intended for use in armed conflict. These laws grew significantly during the Cold War, as Western bloc states sought to restrict the flow of defence technologies to the Eastern bloc.[154] These export limitation regimes also apply to 'dual use' goods: sensitive products that have legitimate uses in both peace and war. Products that embody certain cryptographic functions can fall into this dual use category.

Prior to the 1990s, the US (and other states) regulated the export of strong cryptographic products with an extremely broad brush. Export prohibitions were framed in such expansive language that almost any export required prior government licence. At the beginning of the 1990s, the implementation of strong cryptography in software for general purpose computers, the growing body of non-governmental research work into cryptography, the availability of the Internet as a means to distribute know-how and source code, and the increasing pressure for reliable standards-based cryptographic implementations in support of cyberspace infrastructure, collided with these same export restrictions.

In the US, a series of legal actions under US free speech law were brought challenging the validity of export regulations as applied to cryptographic software. The argument presented proceeds, in essence, as follows: source code is expressive, expressive content is protected speech, therefore source code is speech, the export regulations are therefore a governmental prior restraint on speech, as a prior restraint the regulations must be extremely narrowly tailored to address a clear danger, but the regulations are in fact very broadly drawn and therefore do not meet constitutional muster. The

US courts struggled with the concept of whether source code was protectable speech. Eventually, in *Junger v Daley* (2000), the US Court of Appeals for the 6th Circuit held that source code was speech and found the US export regulations unconstitutionally over-broad [154].[155] No doubt in response to this and similar legal challenges in other US Circuits, combined with heavy lobbying by the ICT industry, the US government issued revised export regulations to create significantly more limited restrictions on cryptographic exports [155].

Many states including the US continue to maintain export restrictions on certain dual use products, including some implementations of cryptographic technology. Anyone engaged in the production of these products should review applicable laws carefully, as violations can be prosecuted as crimes.

11.2 Industry-specific regulations

Various industry regulators embrace cyber security within the framework of their larger role regulating subject industries. Financial services regulators, for example, in their role as regulators of banking operational risk have always had some degree of subject matter regulatory jurisdiction over cyber security measures. Details of cyber security risk management have increased in prominence within the field of financial services regulation and can be expected to continue to feature prominently in this regulation [156].

As states have begun to focus more generally on cyber security risks, the existing industry regulators have been encouraged to bring cyber security into their supervisory and regulatory frameworks especially in the context of critical national infrastructure [157]. This regulation has taken many different forms, and debate continues about different models to regulate cyber security risk management [158].

11.3 Encouraging increased cyber security for products and services

The emergent Internet of Things and the accompanying growth of cloud-based services creates increased risks from cyber security breaches to both consumers and business enterprises. Policy makers have begun to adopt legal frameworks for certification of compliance of products and services with various cyber security standards. In the European Union, certification activity is expected to operate within the framework of the EU Cyber Security Act [159]. (See also discussion of certification marks used by public and private standards bodies in section 8.2.3.)

11.4 Matters classified as secret by a state

Practitioners who are employed or engaged by states are routinely subject to laws that mandate secrecy of certain information classified as secret by those states. Most commonly, this arises in an environment where the disclosure of relevant secrets could harm the defence of the state, the integrity of a police investigation, the safety or efficacy of persons conducting state sponsored espionage activity, etc.

These laws can sometimes be used to intervene and classify as secret the research and development work of third parties. Practitioners may also come within the remit of these laws when state security officials choose to disclose certain classified information relating to cyber threats.

These laws tend to authorise extremely severe criminal penalties for those who violate them.

12 Public international law

[9]

Public international law (often referred to more simply as 'international law') is the body of law that regulates relationships among and between states (which for these purposes includes international

governmental organisation). Sources of public international law include treaties, widely accepted international norms and customs, and decisions of international tribunals.

Only states are said to have 'standing' to enforce claims arising under public international law. Non-state persons are normally unable to take legal action against states for violation of public international law. A non-state person may hold the right to take legal action against their home state for failure to implement obligations imposed upon the state by public international law, although states normally have to grant these rights to non-state persons [53].[156]

Similarly, international law normally seeks to regulate the behaviour of states rather than the actions of their residents or nationals.[157] Cyber operations undertaken by a non-state person in State A against persons or equipment in State B normally do not constitute a violation of international law, unless the action can be attributed to State A (see Section 12.1.) This action by a non-state person could, however, serve as a legal justification under international law for State B to launch a proportionate response against such persons or equipment in State A as an act of self-defence (R.4, n.2).

At the time of writing, the most comprehensive source of analysis on the application of public international law to cyber operations in times of peace and armed conflict can be found in the Tallinn Manual 2.0 [9].[158] All citations in Section 12 that take the form '(R.x, n.y)' are references to Rules and explanatory Notes in the Tallinn Manual 2.0.

12.1 Attributing action to a state under international law

Attribution describes when a state is held legally responsible under international law for a given action. Thus, attribution is simply a series of legal doctrines used to define whether or not a state is responsible for a given act (R.14-19).[159]

A given action might be legally attributed to a state if, for example:

- the action is undertaken by an agent or officer of the state (such as an active on-duty member of the state's military or police acting pursuant to orders); or
- the action is undertaken by a non-state person (such as a technology services provider) under the direction, or with the active encouragement, of state officials.

In extreme circumstances, if illicit activity is regularly initiated by non-state actors from cyber infrastructure inside the territory of a state, and that state remains willfully blind to that activity or otherwise fails to exercise appropriate due diligence in attempting to identify and restrain the illicit activity, then it may be possible to attribute the illicit activity to that state. This theory is not without controversy (R.6-7; R.14, n.3).

12.2 State cyber operations in general

Public international law is founded on the principle of territorial sovereignty.[160] A state is said to be sovereign within its own territory, and also has the right to conduct activities outside of its territory consistent with international law.

International law generally prohibits one state from violating the sovereignty of another (R.4). States are, however, entitled to take appropriate countermeasures in response to a second state that has violated the obligations it owes under international law to the first (R.20-26). Countermeasures are actions that would normally violate international law that are directed against the second state in an effort to encourage it to comply with its obligations under international law.

Countermeasures must be proportionate to the complained-of violation of international law by the second state. Although countermeasures against an illegal cyber operation might consist of cyber or

non-cyber responses, this raises a recurring challenge when attempting to understand how to assess the relevant proportionality of a non-cyber countermeasure to a cyber incursion.

A cyber operation of one state directed against another state is normally contrary to the principles of international law if it interferes in the affairs of the second state (R.66). A cyber offensive operation such as a DDoS operation, for example, would constitute interference if used to coerce the second state in a manner designed to influence outcomes in, or conduct with respect to, a matter reserved to the target state (R.66, n.8&19). The outcomes in question need not be physical in nature, and can include domestic political outcomes (R.66, n.20).

A cyber operation of one state directed against another state is normally contrary to principles of international law if it constitutes a threat or use of force (R.68-70).

A state that is victim of an 'armed attack' is entitled to take proportionate countermeasures, including the use of force (R.71). Actions that constitute an armed attack are a sub-set of acts that constitute 'use of force' (R.71, n.6). Finding the dividing line between them is challenging and is generally measured by reference to the scale and effects of the complained-of act. In the context of discussing the Stuxnet operation, for example, the Tallinn Manual 2.0 experts agreed that if this operation were to be attributed to a state it would constitute a use of force but they were divided on whether the scale and effects of the operation were sufficient to constitute an 'armed attack' (R.71, n.10).

When engaged in armed hostilities, state-conducted cyber operations are assessed by reference to the traditional international law applicable to warfare. The Tallinn Manual 2.0 deals with this topic in extensive detail and includes reminders that states must choose their targets with care to avoid targeting, and to minimise injury to, non-combatants.

12.3 Cyber espionage

Cyber espionage, *per se*, is not generally considered a violation of international law (R.32) [57, 58, 160]. Cyber surveillance and evidence gathering activities conducted from within the territory of one state against persons or equipment in another state would therefore not necessarily constitute a violation of international law on their own. Espionage methods, however, could easily violate the domestic criminal law of the second state (e.g., unauthorised access to computers). Furthermore, methods that support espionage by harming equipment or deleting data processed within the territory of the second state would constitute a violation of that state's sovereignty and (if sufficiently damaging) could amount to a use of force.

A specific example of this principle applies to state efforts to tap submarine communication cables for the purpose of intercepting communications. If a state covertly taps cables in international waters without significantly interrupting their functionality, this very likely does not constitute a violation of international law. If one state places the tap within the territorial waters of a second state, however, the operation constitutes a violation of the second state's sovereignty (R.54, n.17).

12.4 Cross-border criminal law investigation and enforcement

Actions by one state that constitute the exercise of police power within the territory of another (unrelated)[161] state normally constitute a violation of that state's sovereignty under international law. This is easy to see in cases where police powers involve the use of force in person, such as searching physical premises, or arresting or interrogating a suspect located in the second state.

States do not generally enforce the criminal laws of other states. They are also not generally required to assist other states with criminal investigation or enforcement (R.13). They may, however, choose to respond favourably to requests for assistance to gather evidence or detain suspects. Rendering this assistance may constitute an international legal obligation pursuant to treaty or may result from *ad hoc* diplomatic agreement.[162] Extradition is discussed in Section 2.3.5.

Assistance usually begins with a request from one state to another state. These requests may be coordinated through international governmental organisations such as INTERPOL, or they might be handled through direct bilateral communications between the effected states. The operational rules of these coordination mechanisms can vary widely.

Acts of surveillance conducted from within the territory of one state that do not involve physical contact by that state's agents with the territory of another state are more complex to analyse. While state remote surveillance actions on their own might not constitute violations of international law (see Section 12.3), state evidence gathering methods (such as covertly taking remote command of a botnet controller or other equipment located on the territory of another state) can constitute a violation of the other state's sovereignty (R.4, n.18) and may also constitute the commission of a crime under the other state's domestic law. Nonetheless, it is well documented that remote cyber surveillance and evidence gathering acts are conducted by the law enforcement agencies of various states from time to time with the express or implied authorisation of the investigating state, and directed against the cyber infrastructure in another, non-consenting, state [22].

13 Ethics

Cyber security practitioners often find themselves operating in positions of trust, where special knowledge and skills potentially give them asymmetric power to influence or disrupt the affairs of their clients or other members of the public. Those who act outside of a specific client relationship, such as product developers and academic researchers, exercise special skills in a manner that could cause harm to a wide variety of third parties. Practitioner activities often take place behind closed doors away from the glare of public scrutiny. This is a volatile mix, where ethical norms might assist in curbing behaviours that abuse positions of trust or otherwise present significant risk to the public.

Early cyber security ethics guidance focused significantly on legal risk management such as liability arising under intellectual property, data protection and privacy laws [161]. Although practitioners should remain aware of laws that apply to their actions, compliance with the law, on its own, may be insufficient to guide a practitioner to ethical action.[163]

As a practice that is generally conducted in the absence of formal state professional regulation, it is difficult to identify generalisable norms that are expected to apply to activities undertaken by security practitioners.[164] This section will survey some of the recurring issues and potential sources of guidance.

13.1 Obligations owed to a client

A review of some obligations normally owed by professionals to clients may be helpful as societies (and various nascent professional bodies) continue to develop approaches to obligations that should be owed by cyber security practitioners to their clients.

At the very least, one can identify various duties of care that arise under contract or tort law to conduct services and other activities that involve risk in a reasonable fashion and with appropriate expertise. Product designers similarly owe various legal obligations under the normal rules of tort law.

Regulated professionals are normally expected to act in the best interests of their clients, to avoid conflicts of interest and to maintain the confidentiality of client affairs. While affirmatively adopting these types of obligation by contract is often non-controversial, difficulties can arise when a security practitioner and client disagree about the most appropriate course of action in specific circumstances.

Challenges can arise with respect to non-mandatory disclosure of evidence to interested third parties.[165] If a practitioner discovers evidence of wrong-doing and there is no supervening legal obligation to report that evidence, the practitioner and client might disagree concerning the disclosure of such evidence to interested third parties such as relevant police authorities, CERTs or tort victims.

These cases can be difficult to navigate. In cases of evidence of economic crimes directed against the client (e.g., petty theft), the client may view public disclosure as more damaging than handling the matter solely on an internal disciplinary basis. In cases where an employee is found to have harmed a third party through tortious action such as negligence, disclosing this evidence to the victim may work to the financial detriment of the client's company through vicarious liability.

Other cases that prove difficult arise when the interests of the practitioner and their client are not aligned. Some professional ethics systems, for example, allow a regulated professional to disclose some parts of a client's confidential information as part of a legitimate bill collecting activity (e.g., by filing a legal action for breach of contract relating to the delivery of confidential services). Such disclosures must normally be limited to information that is necessary to pursue collection and may come with obligations to seek appropriate protective orders from the courts.

Actions by a practitioner that interfere with the proper functioning of their client's infrastructure in an effort to exercise undue influence over the client are unsavoury at best, and might cross a line into criminal conduct at worst. An express or implied threat of such action seems no better.

It remains to be seen whether cyber security practitioner-client relationships will become the subject of formal state regulation or licensure in due course.

13.2 Codes of conduct

Various professional bodies have published codes of conduct and ethical guidelines for cyber security practitioners. Many of these refer to high-level ethical principles without the more detailed guidance that is necessary to assist practitioners with interpretation of the principles.[166]

Examples of two more recent and carefully considered codes of conduct are presented below for consideration. One is framed as a code of general applicability and one is built around a defined business process.

The Association for Computing Machinery can trace its history to the mid-twentieth century and maintains a global membership of more than 100,000 [162]. The ACM Code of Ethics and Professional Conduct was extensively revised in 2018 to take account of the impact of data connectivity [163]. The revised ACM Code provides multiple points of guidance relevant to the field of cyber security. The ACM also provides supplementary materials to assist in understanding and applying the Code [164].

The ACM Code clearly demonstrates the difficulties of balancing ethical imperatives. In its admonition to avoid harm (Section 1.2), it states there is an 'additional obligation to report any signs of system risks that might result in harm'. While the Code addresses the possibility of 'whistle-blowing' as a reporting technique in appropriate circumstances, it also cautions that 'capricious or misguided reporting of risks can itself be harmful. Before reporting risks, a computing professional should carefully assess relevant aspects of the situation'.

By contrast, CREST was established in the UK in the early twenty-first century originally as a membership body for firms who supply penetration testing services.[167] At the time of writing, it has more than 140 accredited member firms [165]. Penetration testing typifies a service that should be of significant concern to the public: information asymmetry means clients are generally unable to distinguish good practice from bad, services are supplied confidentiality away from public scrutiny, and practitioner errors can cause disproportionate harm to clients or third parties. The CREST Code of Conduct for CREST Qualified Individuals provides guidance on numerous topics relevant to delivering these services including service methodology, ethical business practices, and obligations owed to clients [166]. The CREST Code also provides a client complaint mechanism and the organisation reserves the right to expel from membership those who fail to adhere to the CREST Code. To the extent that clients mandate that suppliers of relevant services maintain CREST membership, these mandates may slowly migrate CREST from a purely voluntary membership association into a *de facto* regulator of those who supply these services.

By historical standards, cyber security presents a relatively new set of methods and processes which are at best poorly understood by the public. Generalised codes like the ACM Code are helpful, as they guide a community of persons with relevant technical expertise who may work in fields as diverse as research and development or security management. Service-specific codes like the CREST Code are helpful, as they focus clearly on specific high-risk services. Codes of conduct will undoubtedly continue to develop as the impact of cyber security practitioner activity on the public becomes better understood.

13.3 Vulnerability testing and disclosure

The process of searching for, finding and disclosing security vulnerabilities causes recurring ethical (and legal) issues [167, 168].

13.3.1 Testing for vulnerabilities

Practitioners who test for security vulnerabilities should consider carefully the nature of their activities. The mere act of studying and analysing objects such as tangible hardware products, locally resident licensed software, or published cryptographic primitives and communication protocols, is normally uncontroversial. It is difficult to draw a line of causation from the mere act of analysis to public harm.

Practitioners should be careful, however, to consider the source of the security object under study. There may be a distinction, for example, between reverse engineering a silicon chip to discover the functionality of a trade secret cryptographic scheme and reverse engineering third-party software of suspicious provenance that embodies the same secret methodology. Although the first might be generally permissible, the second may constitute a violation of trade secret rights and result in liability or limitations on one's ability to publish results [140, 141] (see the discussion in Section 8.4.2 and Note 171).

When vulnerability testing is conducted remotely, the testing methods can create further problems. Practitioners must first remain cognisant that unauthorised efforts to gain access to a computer system are often defined as a crime (see Section 5). As stated in the ACM Code Section 2.8, 'A system being publicly accessible is not sufficient grounds on its own to imply authorization' [163]. If practitioners are testing in response to a 'bug bounty' program, they should review carefully the terms of the program to assure that they are not exceeding the scope of authorised testing activity.

Practitioners should also consider the potential impact of their testing methods on the stability of public or private infrastructures, including those that are the target of testing as well as intermediary and third-party systems.

13.3.2 Disclosure of vulnerabilities

Those who find security vulnerabilities face a choice of what to do with their new-found knowledge. Choices exist on a spectrum from making no disclosure, to publishing every detail immediately to the world at large. In between these two extremes lie an array of possibilities.

Those who make no disclosure choose to do so for different reasons. Some wish to make no disclosure in an effort to avoid complicated problems of ethics and potential liability. It is difficult to reconcile this position with the ethical obligation expressed in the ACM Code Section 2.8 'to report any signs of system risks that might result in harm' [163].

Some who operate in support of state security agencies may wish maintain the secrecy of a vulnerability after deciding that the risks and benefits of disclosure outweigh the risks and benefits of maintaining secrecy [169, 170, 171, 172].[168] The ethics of this 'equities' balancing process is a topic of continued debate [171, 173].[169]

Finders who choose to make an immediate full public disclosure of vulnerabilities without any prior warning to any effected person may do so for a variety of reasons. Some suggest that this is the only

certain method of encouraging remediation efforts by developers. Some do not wish to invest in the time-consuming process of staging the private and public disclosures described below. Some fear that engaging with developers will prompt a legal intervention prohibiting disclosure.[170] It is difficult to reconcile these arguments with the guidance from the ACM Code to minimise harm.

Many practitioners follow a principle known as 'responsible disclosure'. The idea is to disclose first on a confidential basis to a person or group of persons who may be able to remediate or mitigate the impact of the vulnerability. After a period of time has elapsed, the finder might then proceed to a second stage of public disclosure. Second-stage public disclosure is often justified by the practitioner on the theory that publication will enable other practitioners to study and avoid similar vulnerabilities, and/or incentivise product and service providers to remediate the vulnerability.

At the time of writing, there appear to be no generally agreed principles on the proper conduct of responsible disclosure. Points of divergence include:

- how to manage private disclosure when the vulnerability forms part of a widely adopted industry standard;
- how to manage private disclosure when the vulnerability is found in a product which forms a component or sub-component in downstream products;[171]
- defining the appropriate length of time between private and public disclosures;
- defining what circumstances, if any, mandate an indeterminate delay to public disclosure; and
- defining how to respond if the finder and developer disagree about the wisdom or timing of public disclosure.

Public disclosure of vulnerabilities could also create tortious liability for a disclosing finder, especially if the process or sequence of disclosures is poorly managed or the vulnerability is misdescribed.

Practitioners who seek to justify publication on the basis that it fits generally within the rubric of 'responsible disclosure' may receive a poor reception from state authorities [140, 141].[172]

Various efforts to obtain financial benefits from disclosing a vulnerability also lead to debate. Accepting a financial reward from a vendor pursuant to a published 'bug bounty' programme seems now to be widely accepted, especially as the vendor controls the terms of the programme. Other more controversial tactics include:

- requesting a financial 'bug bounty' from a product developer or service provider as a condition of disclosure when the relevant party has no existing bug bounty programme in place;
- selling knowledge of the vulnerability to a third-party broker, who then re-sells the information; and
- engaging in market trade activity (e.g., short-selling stock) in an effort to profit financially from advance knowledge of the vulnerability [174].

Practitioners who find vulnerabilities during the course of their work as security researchers must further consider the extent to which they may be accountable to their employer or funder for any financial benefits obtained.

13.3.3 Facilitating and acting on vulnerability disclosures

Product and service vendors should consider how they can facilitate and then act upon vulnerability disclosures in a manner that minimises harm to customers and third persons.[173]

Key principles to facilitate proper vendor handling of vulnerability disclosures include: publishing acceptable methods to disclose vulnerabilities to the vendor, working diligently to verify the vulnerability, developing remediation or mitigation strategies, disseminating fixes, working with supply chain partners, and providing feedback to finders.

A framework to develop specific vendor policies and processes can be found in ISO/IEC 29147 (the process of receiving and handling information about vulnerabilities) and ISO/IEC 30111 (the process of verifying and remediating vulnerabilities) [175, 176]. State agencies have also published varying guidance on this topic, which is revised from time to time [177, 178].

14 Conclusion: Legal Risk Management

Anyone seeking to understand legal responsibility often begins with an information deficit. Simply learning about the many laws and regulations that govern the operation of a single enterprise can be prohibitively time-consuming and expensive.

This problem multiples according to the number of jurisdictions with which a person may be dealing – a significant challenge if cyberspace truly enables contact with every jurisdiction in the world. In the modern era of more than two hundred sovereign states recognised under public international law, plus hundreds of states that are members of a federal or similar structure, plus untold tens (or hundreds) of thousands of additional municipal jurisdictions with varying degrees of law and regulation-making authority, merely discovering the content of the applicable laws and regulations can be a monumental task. Private law obligations imposed by contract and (potentially voluntary) self-regulatory systems complicate matters further. In a field where multinational contacts and relationships are commonplace, considerations of the effective limits of state power are also appropriate.

Compliance with laws and regulations thus becomes a risk management process. What follow are a few subjects for consideration when constructing a legal risk management framework.

Identify subject matter areas of greatest risk. The nature of the activities undertaken by a person (whether business or otherwise), helps to identify which laws and regulations will be of most significance to a given person. For example, banks, telecommunications infrastructure providers, and providers of medical and legal services are always cognisant of their need to seek and maintain appropriate licenses for their activities. Providers of gaming (gambling) services are also very attuned to the wide variation of laws that apply specifically to their operations. And all businesses are extremely cognisant of the need to understand tax reporting, collection, and payment obligations.

Consider the impact on human life. A strict cost-benefit analysis may often be useful when making operational decisions, but becomes problematic where matters of human life and safety are concerned. Laws and regulations adopted to protect human life and compensate for personal injury should be accorded special respect. A blatant disregard of rules that are designed to limit risks of personal injury and death raises significant moral and ethical concerns and can also result in exceptional or punitive measures when these rules are enforced.

Conduct due diligence that is aligned with identified risks. Nobody instructs a lawyer to 'Go and find every law in the world that arguably might apply to anything I do.' A typical due diligence strategy involves first identifying and investigating the laws that could destroy or bankrupt an enterprise. Other laws and regulations may become increasingly significant as an enterprise grows, changes character or makes significant contacts in a new jurisdiction.

Consider the practical limits of territorial enforcement jurisdiction. In the era of online commerce, some enterprises have become paralysed with fear about the potential legal obligations to hundreds

of states whose residents might gain access to site content. Those who remain paralysed may go out of business. Most of the others try to adopt pragmatic approaches that include good faith efforts to filter content in an effort to block the residents of these states from accessing locally-illicit content or products.

Consider the relative cost of breaching a (non-criminal) legal obligation. Committing a crime is different from failing to honour a civil obligation. There are times when the cost of answering a civil legal action is less than the cost of compliance. Most commonly, this occurs in the context of a commercial contract which has become uneconomic to perform, or a civil regulatory requirement with a fixed financial penalty. In appropriate circumstances, a party might reasonably conclude that repudiating its civil obligation (and accepting the risk of a legal action for money damages) is less expensive than fulfilling the corresponding obligation.

Consider the risks to one's own personal reputation, safety and liberty. Cyber security practitioners are sometimes individually confronted with situations where they are tempted, or instructed, to violate criminal law. Those who are tempted to do so should be reminded that they may personally suffer the consequences of their actions, irrespective of whatever incentive has been provided by an employer or client.

Consider the likelihood of enforcement. There are times when persons who have civil legal rights choose not to enforce them. For example, the risk of legal action from an individual natural person who has suffered a de minimis loss as a result of a minor business tort may be diminishingly small. If the rights of thousands or millions of these persons can be joined together in a class action lawsuit, however, the risk becomes enormous.

Consider the challenges of collecting and presenting evidence. The law is not self-executing. Efforts to enforce legal rights and efforts to mount affirmative defences all hinge on one's ability to prove, or to rebut an adversary's efforts to prove, the underlying facts of a dispute. Consider what issues will require proof when an adverse party seeks to enforce a legal right, and how one can collect and preserve evidence to an appropriate forensic standard in anticipation of the need to defend against this effort. Practitioners are also cautioned to explore the parameters of any applicable document or data retention policy, which involves the routine and regularly scheduled destruction or deletion of documents. While the routine destruction of documents in accordance with a carefully defined governance policy is usually permissible, these procedures normally have to be suspended to the extent that the documents may be relevant to any legal action that has commenced or been threatened. Any attempt to destroy evidence that might be relevant to such a legal action often constitutes a violation of the law and can result in severe consequences.

Consider vicarious liability. The only certain way to reduce vicarious liability is to influence employee behaviour to reduce the number of acts that are tortious or otherwise violate applicable regulations. Internal governance documents intended to reduce liability to third parties should therefore be written with the goal of influencing this behaviour.

Consider localising risky activities in separate limited liability legal persons. Lawyers routinely counsel business clients concerning the creation and structuring of separate legal persons in an effort to contain liabilities within defined pools of investment capital. This is a complex subject that requires careful navigation.

Consider risks that are external to the legal system, per se. In some circumstances, the greatest risk arising from a legal action or a threat of legal action has almost nothing to do with laws or regulations, as such. Consider, for example, the impact of a potential legal action on the reputation of an organisation or the impact of an adverse finding on the maintenance of relevant state licenses to conduct business.

Consider changes to law or enforcement policy that are likely to arise. Societies and policy makers are generally becoming more aware of the impact of cyber security. As this awareness increases,

states and their agents may increase enforcement activities, re-examine assumptions about existing policy, and intervene rapidly with amended or new laws.

CROSS-REFERENCE OF TOPICS VS REFERENCE MATERIAL

	goldsmith2006controls [1]	schmitt2013tallinn [9]	kohl2017information [12]	murray2016information [13]	walden2016computer [22]	eu2018handbook [68]	edpb2019guidelines [69]	beale2018chitty [100]
2 Jurisdiction	X		X	X				
4 Data protection			X	X		X	X	
5 Computer Crime					X			
6 Contract			X	X				X
8 Intellectual property			X	X				
9 Internet intermediaries			X	X				
12 Public international law		X						

NOTES

[1]Civil procedure governs process-related matters in non-criminal legal proceedings, such as the form of pleadings submitted to the court (including the size and shape of paper on which they are written), time allowed for defensive pleadings and replies, methods of serving notice on parties, expanding or contracting the number of parties in a law suit, the scope of mandatory disclosure of potential evidence, case management orders, methods of appealing adverse decisions, etc. Examples of these rules can be found in Title 28 of the United States Code, the [US] Federal Rules of Civil Procedure, and the [England and Wales] Civil Procedure Rules.

[2]Criminal procedure governs process-related matters in criminal proceedings. Because criminal proceedings place at risk the individual liberty of the accused, these rules are heavily influenced by human rights law, can be significantly different from civil procedure, and thus are often maintained separately from civil procedure rules. Examples of these rules include the 'Bill of Rights' in the US Constitution, Title 18 of the United States Code, the [US] Federal Rules of Criminal Procedure, the [UK] Criminal Procedure and Investigations Act 1996, etc.

[3]Rules of evidence govern the presentation and examination of evidence before a tribunal. This can include matters such as the prohibition of some categories of hearsay evidence, presentation of so-called 'computer evidence', introduction and examination of expert testimony, permissible examination and cross-examination techniques, etc.

[4]Cyber security practitioners are not alone in this respect. Highly experienced and well-educated lawyers routinely require guidance from 'local counsel' who are retained specifically to assure compliance with these rules when attempting to manage multi-state disputes.

[5]See Note 11

[6]Anecdotal evidence gathered by the author over many years of ICT-focused international commercial legal practice, however, strongly suggests that many of the norms expressed in this knowledge area are also reflected in systems of civil law (see Note 12). There is no claim that the norms presented here would necessarily be found in other, less common, systems of domestic law such as those founded on religious doctrine or *sui generis* customary law.

[7]This concept of evolution in values and the law is not universally accepted. Some systems of law persist in the belief that they are seeking universal truth and reject any other notion as inappropriate or heretical.

[8]The nature and challenges of legal scholarship have been nicely summarised by David Feldman, Q.C. [179]

[9]The pace of change in various laws depends upon how deeply rooted they are in social values. Certain foundational principles concerning the administration of justice (e.g., the right to notice and the right to present one's case to a tribunal), are so slow to change that they appear within the span of a single generation to be immutable. Other types of law (e.g., tax law) are amended continually.

[10]Indeed, the relative utility of a system of law arguably depends upon this characteristic of predictability of outcome. A contrary, perhaps nihilistic, view of law and legal analysis can be found in the academic school of critical legal studies. A good and accessible example is the scholarship of Girardeau Spann [180].

[11]Common law systems are those derived from the law of England. These are the foundation of legal systems in states that had close (usually colonial) historical connections with the British Empire, including England, Wales, Ireland, Australia, New Zealand, Singapore, most of the constituent provinces of Canada, most of the constituent states of the United States, etc. As a result, this system of law is nearly ubiquitous in anglophone territories.

[12]Civil law systems are those derived from a mix of Germanic, Napoleonic, and/or Nordic laws. These are the foundation of legal systems throughout Europe (with the exception of a few common law jurisdictions) and in states that had close (often but not always colonial) historical connections with continental Europe. These include European states such as France, Germany, Italy, Sweden, and Russia, and non-European states such as Argentina, Brazil, Mexico, and Japan. (In the case of Japan, the late 19th century Meiji State selected the civil law of Germany as the primary basis for its legal modernisation programme [181].)

[13]See discussion of 'code' in the text accompanying Note 18

[14]In the author's experience, mistaking a 'bill' (not law) for a 'statute' (law) is not an uncommon occurrence among cyber security practitioners who are unaccustomed to legal research. This is especially easy for the unwary who stumble across the annual mountain of bills introduced by members of the US Congress which never become law.

[15]As a limited narrow exception, some states adopt the practice of examining legislative history (such as the series of draft bills as they were amended in the process of debate to become law) as a means of helping to interpret the law as finally adopted.

[16]The status of European Union legislation in the United Kingdom after Brexit is complex. The UK has already adopted legislation that will generally continue within UK domestic law those EU laws that are most relevant to cyber security post-Brexit (especially data protection regulation), unless and until the UK Parliament decides to diverge from EU legal principles.

[17]In the context of a system of federal states, 'foreign state' can include another member state of the federation. Thus, courts of the State of New York would regard interpretations of law issued by courts of the State of California as the decisions of a foreign state. As such, they would not constitute binding authority in New York State courts, although they might have value as a source of persuasive authority. This discussion should not be confused with the subject of enforcing foreign judgments (see section 2.4.

[18]For example, the United States Code (U.S.C.) (a collection of otherwise disparate Acts of the US Congress organised into code form by editors who then revise the code as further legislation is adopted or amended), and the Bürgerliches Gesetzbuch (BGB) (the comprehensive code of German civil law adopted en masse at the start of the 20th century and amended from time to time).

[19]For example, the Code of Federal Regulations (C.F.R.) (a codified form of US secondary legislation).

[20]E.g.For example, the Uniform Commercial Code (U.C.C.) (a set of model laws produced as a joint project of the Uniform Law Commission and the American Law Institute, which has in turn been adopted with some local variations by most constituent states of the United States and has thus become extremely influential).

[21]This last category can sometimes suggest the future development of law, as states may decide to mandate compliance with codes that began life as suggested rules. Similarly, courts may use advisory codes as a way of interpreting responsibilities such as the requirement to act 'reasonably' in assessing negligence liability.

[22]For example, The Tallinn Manual (a restatement of public international law applicable to cyber operations) and the Restatement (Third) of Torts: Products Liability [9, 112].

[23]Some creative arguments against this result include attempting to recharacterise cyberspace as 'territory' that exists separately from sovereign states, thus attempting to describe a universal and harmonised set of legal principles that should be applicable to all uses of cyberspace globally, and in some cases rejecting the authority of sovereign states to intervene in cyberspace-related activities. The best of these constitute interesting experiments in legal philosophy [182]. More often, they take the form of an anti-state polemic with little or no foundation in legal theory or the reality of modern enforcement practice [3].

[24]This definition of 'proof' stands in sharp contrast to a mathematical proof. In the field of mathematics, to 'prove' something means to establish undeniability as a logical necessity – to establish the truth of a proposition beyond any dispute. (For example, proof of Pythagoras' theorem.) The proof of a real-world event in a court of law never results in absolute certainty. A fact finder in a legal proceeding must reach a conclusion on less than total certainty. A technology journalist eloquently summarised this when he stated, 'The purpose of law is not to achieve philosophical or mathematical truth, but to take a messy reality and achieve workable results that society can live with' [183].

[25]Although courts may use this same phrase to describe the two standards, they remain free to define them differently in the context of interpreting two different laws.

[26]Various financial fraud crimes are often defined in this fashion, for example, requiring that proof that the accused had a specific intention to deceive (*scienter*). Many of the computer crimes discussed in section 5 do not require such proof.

[27]Criminal intent (or its lack) should be distinguished from circumstances where the law expressly provides an affirmative defence such as 'public interest', 'public necessity', or 'self-defence'.

[28]'Civil law' in this context, meaning non-criminal law, should not be confused with the term 'civil law' as a means of classifying systems of law such as are found in the states of continental Europe. See Note 12.

[29]This term can also be used to describe subject matter and territorial authority of legal persons created by treaty between states, such as international governmental organisation (e.g., the ITU) and special purpose multi-state municipal organisations (e.g., The Port Authority of New York and New Jersey, and the Washington [DC] Metropolitan Area Transit Authority).

[30]By contrast, 'subject matter jurisdiction' refers to the scope of the subject matter that can be addressed by a given entity. For example, a single state might choose to divide its court system into two parts: one that addresses only criminal complaints and one that addresses only civil matters. While the territorial jurisdiction of both courts might be identical, the subject matter jurisdiction is clearly different. Similarly, the scope of authority delegated to individual regulatory agencies, ministers of state, etc., constitute a type of subject matter jurisdiction for that agency.

[31]A good introduction to the principles of juridical jurisdiction for civil cases is found in the recast Brussels I Regulation, which presents the rules normally applicable to civil matters in courts located within the European Union [184].

[32]To take an admittedly whimsical fictional example from the Wild West, in the film Silverado Sheriff Langston (portrayed by John Cleese) discontinues his hot pursuit of criminal suspects through the wilderness after a sniper opens fire at his posse. He justifies his action explaining wryly to his companions, 'Today my jurisdiction ends here' [185]. Sheriff Langston's quandary illustrates the relationship between state power and enforcement jurisdiction. Non-fictional examples that explore the territorial limits of state enforcement power are readily available, albeit controversial, and in some cases are the subject of diplomatic and international legal dispute.

[33]See various US statutes criminalising acts of homicide against US nationals while overseas codified at 18 U.S.C. §2332.

[34]Reasons this activity might not be illegal under the law of the first state include, most obviously, where the first state has not adopted any law to criminalise the complained-of hacking activity. Alternatively, the first state may criminalise the activity in normal circumstances but officially warrants the cyber operation pursuant to the lawful domestic authority of the first state. In this second scenario, the person undertaking the operation would normally be immune from criminal prosecution in the first state but subject to criminal prosecution in the second. This discussion focuses solely on liability of the relevant non-state person undertaking the cyber operation. The liability of states to one another for such operations is addressed in public international law (see section 12).

[35]The subjects of espionage and remote evidence gathering are discussed in Sections 12.3 & 12.4

[36]The 1998 dispute over legal control of DNS root servers, and its informal albeit dramatic resolution, is recounted by Goldsmith and Wu and criticised by Froomkin among others [1, 186].

[37]A bank in this situation faces the practical problem of two competing states making conflicting demands: one ordering payment, and a second prohibiting payment. Taking the analysis one step further, imagine what could happen if (in an effort to avoid adverse enforcement actions by the United States) the London branch of a US bank refused to comply with the judgment of an English court. This bank might jeopardise its ability to conduct regulated banking activities in London. Presumably, the depositor could also ask English courts for enforcement assistance by demanding the seizure and forfeiture of funds held by such defaulting US banks on deposit with other banks in the UK. The depositor could also take the judgment and request enforcement by third-party states where the US bank also held funds on deposit. These are the types of analysis that arise when a non-state person considers the risk of potentially conflicting state mandates.

[38]In the context of the US federal system, each member state of the US is normally required to enforce civil judgments issued by courts of other member states under the Constitutional mandate to give 'full faith and credit' to acts of other US states. (US Constitution, Art IV, Sec 1.) A similar rule applies in the European Union by operation of Chapter III of the (recast) Brussels I Regulation [184].

[39]To avoid a point of occasional confusion, police officers are normally able to arrest persons in an airport or other port of entry even if the arrested person is merely transiting the state en route to a third state without requesting entry to the territory of the arresting state. Criminal suspects can be, and have been, arrested in the international transit areas of airports.

[40]One should not assume that the persons who write the (technological) code are the same persons who create the norms to be enforced. As one author has stated, legal analysis has generally moved 'from "Code is Law" to "Law is Law"' [58].

[41]The significant role undertaken by various platform operators in filtering content on a state-specific basis and supplying similar geo-filtering tools to their content supplying customers, is often overlooked in policy debate.

[42]An example of collaborative filtering is found in the work of the Internet Watch Foundation. Among other things, the IWF maintains a URL database of sites known to host images of child sexual abuse. This database is used by various service providers to restrict access to these sites [187].

[43]The opinion of Judge Lynch, concurring, is especially interesting as he wrote to highlight many of the more unsettling and counter-intuitive policy aspects that would result from the judgment and 'to emphasize the need for congressional action to revise a badly outdated statute'.

[44]Although the Microsoft case was dismissed prior to judgment, the extensive collection of briefs filed with the US Supreme Court by a variety of interested third parties constitutes a treasure trove of analysis and advocacy on this topic. It remains possible that a future dispute might be brought in the US courts to challenge the authority of the US Congress under the terms of the US Constitution to extend jurisdiction in this fashion. While the outcome of any such future challenge is debatable, it seems unlikely to succeed.

[45]State-mandated disclosure might arise from processes as diverse as state security intelligence gathering, police investigation, or orders to disclose evidence in civil or regulatory disputes.

[46]The quoted language, with emphasis added, is taken from [188].

[47]Although people most often discuss the issue of data sovereignty in the context of compelled disclosure of data, other state interventions may also be possible such as compelled data alteration or deletion, or compelled service suspension.

[48]Efforts to mitigate this risk using cryptographic technology, database sharding over servers in multiple states, etc. are outside the scope of this knowledge area.

[49]The Regulation, of course, does not interfere with any data localisation rules imposed for reasons of state security as this subject area falls outside the regulatory subject matter jurisdiction of the European Union.

[50]To understand the legal context of the international instruments cited, see the introductory discussion of public international law in Section 12

[51]The conditional nature of the right expressed in Article 7 is explained in an accompanying report [189].

[52]In the US legal system, for example, the Fourth Amendment to the US Constitution provides a set of rights that limit only state actions, while the California Constitution grants a general right of privacy effective against state and non-state actions within its territory. Both the US and its constituent states have promulgated a large number of laws that regulate intrusions under various conditions. The landscape is complicated.

[53]Examples made possible by the emergent mobile app economy include processing data concerning identity of personal contacts, calendar and scheduling information, banking data and authentication credentials, personal notes and communications, browsing and shopping history, intimate relationship data, and a variety of health-related data from heart rate and exercise patterns to menstruation data. Each new data set presents a question about the 'normal' expectation of privacy when using these services, and the permissible scope of intrusion by state and non-state persons

[54]In the referenced case of Smith v Maryland, the US Supreme Court decided in 1979 that compelled disclosure of customer dialling records did not constitute a 'search' for purposes of the Fourth Amendment to the US Constitution as the customer had no expectation of privacy in the list of numbers dialled [56].

[55]Compare the information that can be inferred after discovering that a target of investigation has navigated to a URL string such as 'web.example.com/politicalpartyname/how-to-renew-my-membership.htm' with the discovery that the same person dialled a phone number such as '1-202-555-7730'. In this example, the URL metadata leads to a strong inference of communication content and the probable ability to reconstruct accessed content precisely.

[56]The US Supreme Court, for example, decided as recently as 2018 that a cell phone customer has a reasonable expectation of privacy in location data and therefore the state-compelled disclosure of this data constitutes a 'search' for Fourth Amendment purposes [190]. In Europe, customer location data has been expressly protected under privacy and data protection laws for some time.

[57]Consider, for example, the capability of various de-anonymisation techniques that can be applied to metadata.

[58]There are, of course, risks associated with the implementation of these facilities and examples of how they have been abused in violation of applicable law. Anti-abuse measures are founded on both technological and organisational controls.

[59]In an effort to navigate potential restrictions on reporting new types of interception, some service providers adopted the practice of publishing so-called 'Warrant Canaries' – a statement published on a recurring basis that no interception warrants of a given type had been received. The theory behind this practice was that a subsequent failure to re-publish the Canary would allow the public to infer (without the communication provider expressly stating) that state-warranted interception had commenced. This practice seems to have fallen into disfavour, probably aided by the sometimes-debatable legal status of the practice plus additional state legal interventions that made this strategy more difficult or impossible to carry out within the terms of applicable law. See, e.g., 50 U.S.C. §1874(a) [191].

[60]In the US, some courts have held that efforts to compel disclosure of passwords triggers scrutiny under human rights law as it forces the accused to give testimony against himself, while mandatory presentation of a fingerprint to unlock a

device does not trigger this same legal objection [63]. This is an area where legal standards remain murky and the topic is ripe for further dispute and development [64].

[61] An example is s.49 of the (UK) Regulation of Investigatory Powers Act 2000.

[62] Practitioners should be careful to distinguish between activities such as developing a communications protocol, writing software that implements a protocol, supplying such software to the public, and supplying a service that implements a protocol. A quick test that may assist in clarifying a person's status is to ask this question: 'Would the relevant communications service continue to operate if the processes administered by this person ceased to function?' Thus, a person who supplies IMAP services, SMTP services, or a key distribution service to support end-to-end encryption for a communications app is more likely to be classified as a communications service provider under relevant legislation than a person who merely writes software that implements a protocol. Details of applicable laws diverge significantly and must be investigated on a state-by-state basis.

[63] For example, Brady v Maryland [192]. This is less likely to occur to the extent that the law of a state (such as the UK) prohibits use of intercepted communications as evidence in legal actions [65] at s.56.

[64] The US exclusionary rule has been hotly debated for more than half a century.

[65] Activities undertaken by states in defence of national security generally fall outside the regulatory jurisdiction of the EU, although member states may choose individually to apply similar principles in that context [82], Part 4.

[66] For example, the term 'personally identifiable information' is defined for the purposes of US bankruptcy law at 11 U.S.C. §101(41A) and defined differently for the purposes of a federal law prohibiting the disclosure of video rental histories at 18 U.S.C. §2710(a)(3).

[67] This is a natural result of the US approach to this subject, which is to adopt narrowly drawn *sui generis* laws that specifically focus on individual use cases. The cited decisions are drawn from examples of the US courts interpreting a 1988 law originally adopted to restrict the disclosure of video rental records as they were kept in the 1980s. The courts were called upon to interpret this aging statute in the context of online streaming service records in 2015.

[68] In practice, there may be a strong temptation, and corresponding pressure, to assume that the absence of obvious personal identifiers in a data set means that no personal data is present. A better approach is to appreciate that data protection law tends to measure obligations in proportion to the risks presented by any given processing activity. Data sets with personal data but without obvious personal identifiers might present a lower risk when processed, thus making compliance less onerous in these cases.

[69] The notifications discussed in this section are distinguished from separate requirements, if any, to share security breach information with relevant industry-specific regulators or security coordination authorities (see Section 11.2).

[70] Mandatory obligations to communicate personal data breaches to data subjects irrespective of the risk of harm has been criticised on a number of grounds, including: data subjects become overwhelmed by communications and are unable to distinguish the degree of risk presented by any individual breach, communicating to a large set of data subjects is extremely resource-intensive, and communicating to data subjects could interfere with the ability of police authorities to investigate the breach.

[71] 'The proposed fine relates to a cyber incident notified to the ICO by British Airways in September 2018. This incident in part involved user traffic to the British Airways website being diverted to a fraudulent site. Through this false site, customer details were harvested by the attackers. Personal data of approximately 500,000 customers were compromised in this incident, which is believed to have begun in June 2018. The ICO's investigation has found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information.' UK ICO Statement of July 8. 2019

[72] 'The proposed fine relates to a cyber incident which was notified to the ICO by Marriott in November 2018. A variety of personal data contained in approximately 339 million guest records globally were exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area (EEA). Seven million related to UK residents. It is believed the vulnerability began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems.' UK ICO Statement of July 9, 2019.

[73] The problem is presented in the well-known case of *R v Gold and Schifreen* [193]. The accused were arrested in the UK in 1985 after they had obtained a system password for an early email system and used it to access an email account assigned to a member of the British Royal Family. Although the accused were originally convicted following trial in 1986 for violating the Forgery and Counterfeiting Act 1981, the House of Lords (at that time the court of last resort in the UK) quashed the conviction in 1988 holding that the complained-of action was not a violation of the 1981 statute.

[74] Bruce Sterling provides an interesting history of early computer crime investigation and prosecution efforts in the 1980s by the US authorities, and colourfully describes how they sometimes missed their intended target [194]. Clifford Stoll also describes the contemporaneous challenges he encountered as a private citizen attempting to investigate computer intrusion, complaining that he often could not find law enforcement officials able to assist him [195].

[75]Confusingly, the verb 'to hack' is also used to describe non-criminal, often informal, ICT research and development activities that are pleasingly clever or demonstrate a previously unknown characteristic of an object. This positive connotation of the term now extends beyond the realm of ICT development, as can be found in emerging phrases such as 'life hack' and 'hackathon'.

[76]The role of prosecutorial discretion is one possible explanation for the lack of a *de minimis* exception in the definition of computer crimes. See the discussion in Sections 5.3 and 5.5.

[77]This was discussed after the Click television programme's 'Botnet experiment' was broadcast on the BBC in March 2009, in which the show's producers procured and then commanded the actions of such a botnet, albeit with an avowedly benign intention [196, 197, 198, 199].

[78]In some rare instances, non-state persons are granted the right to bring a criminal prosecution when state officials have chosen not to do so.

[79]This becomes more obvious when considering intrusion efforts against industrial control systems such as those that operate dam sluice gates, national electricity power grids, steel mills and foundries, automobiles, oil tankers, pipelines, and nuclear power generation facilities.

[80]Historically, the Computer Misuse Act 1990 did not contemplate the idea of state-warranted intrusion into information systems. This express exception to criminal liability under the 1990 Act first appeared in the Regulation of Investigatory Powers Act 2000, the predecessor of the Investigatory Powers Act 2016.

[81]Such proof would most likely consist of asking the fact finder to draw reasonable inferences from the circumstances surrounding any given act of production or distribution.

[82]Some have argued that conducting legitimate security research activities should be shielded from most or all criminal and civil liability if appropriate conditions are met [200]. Similar arguments have been advanced in the cause of security-related journalism. These policy arguments have not yet found favour with law makers, although the debate is not well advanced.

[83]It has been suggested that persons who engage in security research and development activity that might otherwise constitute a *de minimis* violation of computer crime laws might enter into formal or informal agreements with law enforcement or state security officials to receive an assurance of non-prosecution. Risks to the practitioner include potential misunderstanding with state officials, potential inability to enforce the non-prosecution agreement, or collateral legal risk such as tort liability [97]. Risks to a state pursuing this strategy include the possibility that such an agreement might be used to attribute responsibility to the state under public international law for the actions of such researchers or developers (see Section 12.1).

[84]In some systems of contract law, however, a service provider may be required to give customers additional time to pay or special notices before services can be suspended. Suspension of services in circumstances that would cause a threat to human life and welfare (e.g., energy services supplied in a freezing cold climate) are often separately regulated and can be suspended only in accordance with strict rules.

[85]Indicia of enforceability are generally beyond the scope of this work. It is both difficult to describe generalisable multinational legal norms about these, and this topic is of lesser concern to cyber security practitioners.

[86]The term 'offer' must be considered with care and distinguished from less significant forms of communication such as an 'invitation to treat' or 'invitation to tender'. While some ecommerce systems make contractual offers to a wide range of potential customers, the most common design is for the vendor to publish invitations to treat – essentially asking customers to make an offer when placing an order. This generally shifts who has control over the time of contract creation back into the hands of the online vendor – an often-useful risk management device.

[87]In this context, 'order' refers to a communication by a potential customer to a supplier seeking a contract. In practice, an order usually constitutes either an offer or an acceptance depending on the terms and conditions applicable to the relevant online platform. In the field of B2C online commerce, it has become common practice for an order to be defined as a contractual offer – capable of being accepted or rejected by the online supplier.

[88]The rule embodied in Article 11 is a rather muted result of a European debate in the 1990s concerning whether to harmonise the time of the contractual trigger in online commerce. Law makers, facing a wide variety of contract rules which are beyond scope of this knowledge area, ultimately chose not to harmonise this aspect of law. The resulting version of Article 11 is limited to this question of defining the time of receipt of electronic orders and acknowledgments.

[89]For example, financial transaction systems such as SWIFT, airline reservation systems such as Amadeus, Galileo, etc.

[90]Codified in 15 U.S.C. §1681c(g).

[91]This knowledge area will not seek to differentiate between a contractual warranty and a contractual condition. Although these create different rights in the hands of a party suffering a breach, the topic is beyond scope of this knowledge area.

[92]Under English law, this is normally styled as the condition of 'satisfactory quality' and was formerly known as the condition of 'merchantable quality.' Under the law of most US states is it styled the warranty of 'merchantability'. Civil law systems adopt a similar concept.

[93]In the law of England and most US states this is styled 'fitness for purpose'. Once again, in England this is said to be a contractual condition and in US states it is generally a warranty.

[94]Examples of typical language found in contracts for the supply of software include, 'Vendor warrants that the software will comply with the Documentation for a period of 60 days following delivery.'

[95]These are not legal terms of art, but merely used to illustrate the variable degree of breach severity.

[96]The names of the remedies are drawn from common law practice. Other legal systems may employ different terms and/or grant alternative remedies.

[97]Those who deal regularly with procurement agreements might find this concept expressed in clauses that specify the right to terminate a contract following 'material breach', 'material breach that causes significant harm', 'a series of minor breaches that collectively create material harm', etc. The definition of the trigger is limited only by the imagination of the drafter, although some legal systems impose limits on the effectiveness of these clauses.

[98]The leading case on this issue in England in the early twentieth Century concerned the duty of a person who bottles beverages owed to those persons who eventually drink them. The advent of the modern economy created supply chains in which the producer and consumer had no direct business relationship, where products change hands multiple times before being consumed. Applying an earlier version of the rule described above, the English court (acting in its capacity as a common law policy maker) stated that the bottled beverage was itself the proximate link between producer and consumer, and that a producer of such a drink could readily foresee the harm caused by the adulteration of the bottle's contents.

[99]A well-known, bordering on comic, example can be found in the 1928 Palsgraf case [201]. (See also discussion of causation in Section 7.3.)

[100]This last category is mentioned because of the occasionally encountered practice where a person attempts to avoid liability by purposefully avoiding knowledge of risk. This strategy is unlikely to defeat a claim of negligence and may even exacerbate liability in jurisdictions that award punitive damages. (See the discussion in Section 7.4.)

[101]In the cited 2018 *Dittman* case, the Pennsylvania Supreme Court announced that the common law of Pennsylvania imposes a duty of care on employers to safeguard the electronic storage of employee data. A mid-ranking appellate court in the State of Illinois reached the opposite conclusion in 2010 when interpreting the common law of Illinois [202]. In the US, negligence law may play an increasing role in defining responsibilities to safeguard personal data.

[102]Judge Hand surprised legal practitioners of the day by expressing this concept using a mathematical formula, stating that if 'B<PL' then the failure to adopt a given method constitutes negligence, where 'B' is the burden (cost) of the method, 'P' is the probability of loss in the absence of the method, and 'L' is the amount of loss to be avoided. These two cases and one formula have been the subject of extensive comment, debate and analysis by generations of US lawyers and law students [109, 111].

[103]In the referenced case, the negligence per se claim was based on an allegation that Target had failed to comply with a Minnesota law concerning the proper storage of credit card details [106]. (See also the discussion of this case at section 7.4)

[104]The Morris worm might be an early example of this type of incident [195].

[105]This section is addressed primarily to 'design defects' and does not discuss 'manufacturing defects', in which individual products from a production run deviate from their specification due to sporadic intermittent errors in the manufacturing process.

[106]Even if a producer of software is not amenable to a claim founded on a theory of strict liability, it could still face a claim founded on a theory of negligence. A victim taking legal action against a software producer based on a theory of negligence would need to prove unreasonable conduct by the software producer.

[107]Such attenuated chains of causation are a familiar meme in science fiction stories about time travel. A non-fiction but entertaining exploration of highly attenuated chains of causation from scientific history is found in the work of journalist James Burke in various iterations of his BBC television programme, 'Connections'.

[108]See also discussion of foreseeability in Section 7.1.1.

[109]Such 'negligent mis-statement' cases are watched closely by professionals and other service providers in the business of supplying critical information-related services such as public accountants. This type of negligence theory is also of special interest to providers of trust services, as it potentially defines their liability to third parties who rely upon the accuracy of issued certificates. (See Section 11.3)

[110]In the cited *Dittman* case the Supreme Court of Pennsylvania, acting in its role as interpreter of the common law of Pennsylvania, held in November 2018 that employers owe a duty of care to their employees to maintain reasonable cyber security to safeguard employee data from loss [107]. In any similar incident in the EU, a tort action could be fashioned easily under a theory of breach of data protection rights.

[111]An obvious example is the various legal actions brought by financial institutions against Target following its well-known 2013 loss of card data incident. Plaintiff banks in at least one of the actions based their claim on various legal theories

including negligence and negligence per se [106]. Settlements of this law suit and others brought by financial institutions against Target exceeded US$100 million [203, 204].

[112] *Compare* easily quantifiable losses resulting from breach of privacy such as loss of revenue from an exclusive agreement to publish the victim's wedding photographs in a specific newspaper, loss of salary as a result of victim's dismissal from employment etc., *with* more difficult-to-quantify harm such as the victim's embarrassment or shame.

[113] This provision is codified in Illinois law at 740 ILCS 14/20.

[114] The internal auditor was arrested and charged with criminal violation of data protection law, computer crime, and fraud. He was convicted and sentenced to eight years imprisonment.

[115] The Supreme Court of the United Kingdom granted leave to appeal on 15 April 2019. Hearing has been scheduled for late 2019, which suggests a possible decision in early to mid 2020.

[116] *Compare* potential application of the state-of-the-art defence in the context of materials science where (for argument's sake) at the time of production there was no known scientific test for the later-discovered defect in the material, *with* the context of a software-induced product defect due to a previously unknown zero day exploit. The former might be said to have been undiscoverable, while the latter was merely undiscovered. It is debatable when a given exploit could be truly classified as having been 'undiscoverable'. This topic merits further study [205].

[117] It has been suggested anecdotally that some regulation of safety-critical systems can lead to weaknesses in that system's cyber security by limiting or foreclosing the possibility of adopting state-of-the-art security measures. A specific instance related to the author concerns a regulatory requirement that certain safety-critical control systems must be exhaustively tested by examining every possible state of the control device prior to use. Some defensive cyber security methods, especially those that adopt artificial intelligence or machine learning, are by their nature impossible to test to exhaustion in this fashion. This topic merits further study.

[118] A favourite example beloved of law professors involves the hypothetical case of the badly loaded railroad car. The car may have been improperly overloaded in State A, but only produces injury after the train begins to descend a steep grade many hours later in State B.

[119] This is attributed to US Supreme Court Justice Joseph Story, who apparently used the phrase more than once [206]. A darker shadow was cast over the practice of IP law by Lord Esher, MR, when in 1892 he observed, 'a man had better have his patent infringed, or have anything happen to him in this world, short of losing all his family by influenza, than have a dispute about a patent. His patent is swallowed up, and he is ruined. Whose fault is it? It is really not the fault of the law: it is the fault of the mode of conducting the law in a patent case' [207]. Little has changed in the intervening century [208].

[120] In United States law, copyright comes into existence automatically but must be registered prior to commencement of any US infringement proceedings.

[121] Moral rights arising under an author's rights (*droit d'auteur*) infrequently present challenges for security practitioners and is beyond the scope of this work.

[122] The US fair use exception and other limitations are codified in 17 U.S.C. §107, et seq. Limitations to UK copyright are codified in Chapter 3 of the Copyrights Designs and Patents Act 1988, ss.28, et seq.

[123] The implementation of this protection has proven both inconsistent and controversial [122, 209]. It is codified in US copyright law at 17 U.S.C. §1201, et seq., and in UK copyright law in Part VII of the Copyrights Designs and Patents Act 1988 at ss.296, et seq.

[124] The European Union is in the process of adopting the Unitary Patent, a single patent right that applies throughout much, but not yet all, of the territory of the EU. The status and use of this new patent right continues to evolve.

[125] Inventors should not confuse this concept from patent law with various scientific or academic definitions of significant or trivial. A scientifically trivial step can still be 'inventive' in patent law [210].

[126] The phrase 'as such' should serve as a warning that loopholes are about to appear, as if by magic. They are.

[127] While copies of patents and published applications from many states are now easy to find online, correspondence with the patent examiners and the prosecution history is often more difficult to obtain and may require assistance from a legal practitioner. Once obtained, however, this can be very enlightening to any person who wishes to challenge *post-facto* the validity of a granted patent.

[128] A very limited subset of patent applications for inventions are subject to a state secrecy classification and are only published in a register of secret inventions.

[129] Anyone innovating in the ICT field faces a series of related challenges. The pace of ICT innovation is so fast, the intermingling of parallel innovative ideas so commonplace, the number of patent applications filed so large, and the prior art cataloguing ICT innovation so untidy, that it is difficult to produce any innovative ICT product that does not infringe some extant third-party patent, or published or unpublished application. A typical strategy adopted by large ICT developers is to file large numbers of patent applications on their own inventions, move to market as quickly as possible with new products,

and then wait to receive suggestions of patent infringement from third parties in the hope of eventually defending against some of these threats or negotiating an acceptable cross-license arrangement.

[130] In the US patent system, awareness by the infringing party of patent rights triggers a special 'treble damages' rule: monetary damages awarded to the rights holder are multiplied by three with effect from the date of the infringer's awareness. This is why rights holders typically begin a US patent enforcement process by sending copies of their patents together with a 'we wish to make you aware' cover letter that does not expressly accuse the recipient of infringement. This, combined with the factors set out in Note 129, is why many ICT innovators assiduously avoid researching third-party patents and patent applications.

[131] Some states define 'unregistered' trademark rights which are similar in character to the English law tort of passing off.

[132] A Community Trademark is a single trademark that extends throughout the territory of the EU.

[133] In modern trademark practice, the relevant sign can consist of sounds or smells. A sound trademark likely to be familiar to cyber security practitioners is the 'Intel Inside' musical chime (US75332744, UK00002403603).

[134] Trademark UK00000000001 has been registered continuously in the UK from 1876 to date.

[135] Courts are divided on the question of whether meta-tags, not normally visible to end users, can constitute an infringement of registered trademarks. Even where meta-tags cannot be used to prove infringement, they can serve as useful evidence for other purposes such as demonstrating the knowledge or awareness of the tag author in related tort actions such as passing off.

[136] By contrast, in actions based on theories of passing off or unregistered trademark rights the complaining party is usually required to prove that the accused party has knowledge of the unregistered mark and is purposefully taking advantage of the reputation connected to that mark.

[137] An example that should be familiar to practitioners is the Wi-Fi logo (US75799630, UK00002209133) registered by Wi-Fi Alliance.

[138] A commonly-cited example of a long-standing trade secret is the formula for Coca-Cola, which remains the subject of much speculation.

[139] 17 U.S.C. §1204(a).

[140] Copyrights Designs and Patents Act 1988, s.296ZB.

[141] The European Union Directive does not mandate the criminalisation of trade secret misappropriation [129]

[142] Note that the Ecommerce Directive does not apply to data protection law [101] at Art 5(b).

[143] For example, 17 U.S.C. §512 (shielding from copyright infringement), 47 U.S.C. §230 (shielding from liability those who block or screen offensive material, although not applicable as a shield against liability arising under obscenity, IP or privacy laws.) Section 230 in particular has come under increasing scrutiny by US courts as more legal actions have been taken against social media service providers.

[144] Although these legal definitions are not specifically linked to technical definitions, this concept is approximately equivalent to providing services that consist of nothing more than carrying and routing traffic at the physical, data link and/or network layers of the TCP/IP protocol suite. A good definition of the concept is found in Article 12 of the Ecommerce Directive [101].

[145] See Article 14 of the Ecommerce Directive [101].

[146] The best-known procedure codified in law is probably found in US copyright law at 17 U.S.C. §512(c).

[147] The 'Allow States and Victims to Fight Online Sex Trafficking Act of 2017' is the result of the FOSTA-SESTA bills proposed in Congress. The narrowing of the liability shield is codified in 47 U.S.C. §230(e)(5). A legal action challenging this law as a violation of US freedom of speech principles was launched shortly after its passage and remains pending at the time of writing [211, 212].

[148] By underwriting the risk of many such transactions, the positive impact of the payment card industry to the growth and success of these platforms should not be underestimated.

[149] The 'three-corner' model for this purpose comprises only three persons: the certificate issuer who both identifies the signatory and issues the certificate, the signatory whose identify is bound to the certificate and the third party who relies on the certificate to identify the signatory. As each of these operational steps becomes divided between more persons, analysing the relationships and responsibilities becomes more complex.

[150] See, for example, X.509.

[151] These doubts tend to arise from a combination of legal doctrines, such as a failure to form a contract as a result of failing to communicate the terms or a refusal to enforce limitations of liability due to public policy concerns such as the reasonability of the limitation or consumer protection. Note that these concerns are more easily addressed in the so-called

'two-corner' issuance model, where a signatory self-certifies its identity and serves as its own certificate issuer. In the two-corner model there is no 'third party' and the signatory may have a direct relationship with the relying party more easily enabling the imposition of liability limits.

[152]Stephen Mason's work in particular includes an extensive international catalogue of these laws [150].

[153]A similar analysis could apply in circumstances where enterprises order their members of staff to adopt and install trust certificates issued by the enterprise specifically to support SSL/TLS inspection. These enterprises should consider the various types of liability that might arise as a result.

[154]States may also apply embargoes on most or all trade with specific states as part of a more general programme of sanctions.

[155]The precise status of software as speech for purposes of US free speech law remains somewhat murky. While US Federal courts seem willing to classify source code as protectable expression, they also appear to take its inherent functionality into account when assessing free speech rights, which in turn suggests that government intervention to restrict acts of distributing source code are more easily justified than restrictions on classic non-functional speech [155, 213, 214].

[156]In the referenced Halford case the complaining party successfully argued that the United Kingdom had failed to provide her with privacy rights required by the European Convention on Human Rights as regards interception of communications by state authorities [53]. This case precipitated the adoption by the UK of comprehensive legislation regulating the interception of communications.

[157]A notable exception involves prosecution according to the principles of international criminal law such as crimes against humanity.

[158]The process of creating the Tallinn Manual was not without controversy [215].

[159]The term 'attribution' is often used in more than one sense. Practitioners should be careful to distinguish the legal doctrines used to analyse attribution from the evidence used to prove satisfaction of the given attribution doctrine. This section discusses only the former. The latter is more properly addressed in the field of forensics.

[160]The principle of territoriality and the exercise of state power is explored in the context of jurisdiction in Section 2

[161]The qualifier 'unrelated' state is meant to distinguish circumstances where more than one sovereign state maintains concurrent jurisdiction over a single territory, as found in federal states.

[162]Among other creative procedures adopted, there have been circumstances where law enforcement officers from one state are allowed to interrogate a suspected cybercriminal on the diplomatic premises of that state's embassy on the territory of the second state.

[163]In the case of offensive cyber operations undertaken at the direction of a state, compliance with 'all applicable laws' may indeed be impossible as the actions taken at the direction of a sponsoring state may constitute crimes under the domestic law of the target state. Similarly, in some circumstances a practitioner might complain that compliance with a legal obligation is, itself, ethically challenging [216]. This section does not attempt to resolve these issues.

[164]Practitioners should be mindful that if they are employed or engaged by a regulated professional firm (e.g., a legal, medical, or public accountancy firm) the practitioner may be obliged by applicable law to conform with the rules of the relevant regulated profession – especially on matters such client confidentiality or client's legal privilege to prohibit the disclosure of sensitive information. These practitioners must become familiar with the obligations imposed by the regulations that apply to that firm.

[165]This discussion does not address circumstances where applicable law mandates disclosure of this evidence to identified third parties, such as the data breach disclosure requirements imposed by GDPR. In such cases, a practitioner should be careful to take appropriate advice concerning their individual legal reporting obligations as distinct from obligations imposed upon their client, and to urge their client to investigate the client's own potential legal reporting obligations.

[166]Many early examples include mandates to 'comply' with the law, while others demand that a practitioner should 'be aware' of the law. Some include the concept of avoiding harm to others without discussing the subtleties of this proscription. Some speak of a general affirmative obligation to protect 'society', without identifying the nature of the obligation in practice, identifying the relevant society in cases where two societies are in conflict, or discussing the possible conflict between protecting society generally and a client individually. Some speak of obligations to protect 'infrastructure', without clarifying whose infrastructure is to be protected: public, private, first-party, third-party, domestic, or foreign. Many of these codes fail entirely to discuss specific obligations owed to a client and how to manage potential conflicts.

[167]CREST has subsequently added additional services to its certification process.

[168]Some risks of disclosure might include the impracticability of patching or fixing the vulnerability. The benefits of secrecy might include a state security agency's ability to exploit the given vulnerability.

[169]Security agencies in the US, UK, and Australia have published some or all of their review processes governing these decisions [170].

[170]This is a special threat for finders engaged in academic security research who face normal academic pressure to publish research results [200].

[171]While disclosing a unique vulnerability in a single online service to a single effected firm is simple, disclosing a vulnerability in a complex supply chain presents special problems. Disclosing first to downstream producers of finished goods or services focuses the disclosure on those who appear to have the most at risk from security failure, but who may not have the tools necessary to mitigate the threat. This downstream disclosure also creates a risk of alienating the upstream developer of the component – especially if the vulnerability is misdescribed. In the field of academic security research in particular, researchers often depend on good continuing relationships with the developer community. Disclosing first to the upstream developer creates a challenge if that developer is dilatory in remediating the vulnerability. Finders in this situation might consider the potential for a multi-step private disclosure process starting (perhaps) with the upstream party most likely to be able to understand and remediate the threat. Having disclosed and then provided an opportunity for that party to analyse or rebut the claim of vulnerability, the finder might begin additional private disclosures one step at a time down the supply chain to those who might take action to mitigate the threat. Second-stage public disclosure would then become a last step of many.

[172]Commenting on a decision by academics to publish vulnerability details more than nine months after private disclosure to an upstream security component vendor, but in the face of strong objections by a downstream product manufacturer, an English High Court Judge noted, 'I think the defendants' mantra of "responsible disclosure" is no such thing. It is a self-justification by defendants for the conduct they have already decided to undertake and it is not the action of responsible academics.' *Megamos Crypto (Volkswagen v Garcia)*, Para 42 [140, 141]. Note that the academics in the *Megamos Crypto* case claimed that they were adhering to responsible disclosure procedures published by the National Cyber Security Centre of the Netherlands, the state in which they conducted the bulk of their research.

[173]While the mere presence of a vulnerability in a product or service does not necessarily constitute vendor negligence, persons who receive a vulnerability report should consider that a failure to act in a reasonable fashion following receipt of a report could constitute an independent act of negligence with resulting liability to parties who suffer foreseeable harm.

REFERENCES

[1] J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World*. New York, NY: Oxford University Press, 2006.

[2] O. W. Holmes, *The Common Law*. Boston: Little, Brown and Company, 1881.

[3] J. P. Barlow. (1996) A declaration of the independence of cyberspace. [Online]. Available: https://www.eff.org/cyberspace-independence

[4] L. Lessig, *Code: Version 2.0*. Basic Books, 2006.

[5] C. Millard and R. Carolina, "Commercial transactions on the global information infrastructure: A european perspective," *The John Marshall Journal of Information Technology & Privacy Law*, vol. 14, no. 2, pp. 269–301, 1996.

[6] D. R. Johnson and D. Post, "Law and borders–the rise of law in cyberspace," *Stanford Law Review*, vol. 48, pp. 1367–1402, 1996.

[7] C. Reed, *Internet law: text and materials*, 2nd ed. Cambridge University Press, 2004.

[8] "Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security," Report A/68/98, UN General Assembly, 2013.

[9] M. N. Schmitt, Ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013.

[10] "Report of the high commissioner for human rights on the right to privacy in the digital age," A/HRC/39/29, United Nations, 2018.

[11] D. van der Linden and A. Rashid, "The effect of software warranties on cybersecurity," *ACM SIGSOFT Software Engineering Notes*, vol. 43, no. 4, pp. 31–35, 2018.

[12] D. Rowland, U. Kohl, and A. Charlesworth, *Information Technology Law*, 5th ed. Routledge, 2017.

[13] A. Murray, *Information Technology Law: the Law and Society*, 3rd ed. Oxford University Press, 2016.

[14] "American Banana Co. v. United Fruit Co." 213 U.S. 347 (US S.Ct), 1909.

[15] "United States v. Alcoa," 148 F.2d 416, 2d Cir. sitting by designation of the US S.Ct, 1945.

[16] "Wood Pulp," 1988 ECR 05193, 1988.

[17] J. J. Friedberg, "The convergence of law in an era of political integration: The wood pulp case and the alcoa effects doctrine," *U. Pitt. L. Rev.*, vol. 52, pp. 289–326, 1991.
[18] "Foreign Corrupt Practices Act," US Statutes, vol. 91, pp. 1494-1500, 1977.
[19] "Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA," *Official Journal of the European Union*, vol. L 335, pp. 1–14, 2011.
[20] "PROTECT Act," US Statutes, vol. 117, pp. 649-695, 2003.
[21] "LICRA v Yahoo! Inc & Yahoo France," (Tribunal de Grande Instance de Paris, 22 May 2000), affirmed in LICRA & UEJF v Yahoo! Inc & Yahoo France (Tribunal de Grande Instance de Paris, 20 November 2000), 2000.
[22] I. Walden, *Computer Crimes and Digital Investigations*, 2nd ed. Oxford: Oxford University Press, 2016.
[23] "Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA," *Official Journal of the European Union*, vol. L 218, pp. 8–14, 2013.
[24] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC," *Official Journal of the European Union*, vol. L 119, pp. 1–88, 2016.
[25] "Google Spain SL, Google Inc. v AEPD, Mario Costeja González," C-131/12, ECLI:EU:C:2014:317, 2014.
[26] "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – version for public consultation„" European Data Protection Board, 2018.
[27] K. Kopel, "Operation seizing our sites: How the federal government is taking domain names without prior notice," *Berkeley Technology Law Journal*, vol. 28, pp. 859–900, 2013.
[28] J. Mellyn, "Reach out and touch someone: The growing use of domain name seizure as a vehicle for the extraterritorial enforcement of U.S. law," *Georgetown Journal of International Law*, vol. 42, pp. 1241–1264, 2011.
[29] A. M. Froomkin, "When we say US(tm), we mean it!" *Houston Law Review*, vol. 41, no. 3, pp. 839–884, 2004.
[30] "Libyan Arab Foreign Bank v Bankers Trust Co," [1989] QB 728, 1989.
[31] R. Cranston, E. Avgouleas, K. Van Zwieten, and T. Van Sante, *Principles of banking law*, 3rd ed. Oxford: Oxford University Press, 2018.
[32] R. McLaughlin, "Authorizations for maritime law enforcement operations," *International Review of the Red Cross*, vol. 98, no. 2, pp. 465–490, 2016.
[33] "Twentieth Century Fox and others v British Telecommunications plc," [2011] EWHC 1981, 2011.
[34] P. M. Connorton, "Tracking terrorist financing through SWIFT: when US subpoenas and foreign privacy law collide," *Fordham Law Review*, vol. 76, pp. 283–322, 2007.
[35] "In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation," 829 F.3d 197, 2nd Cir, 2016.
[36] "Stored Communications Act," codied at 18 U.S.C 2701 et seq, 1986.
[37] "CASE NOTE: Privacy — Stored Communications Act — second circuit holds that the government cannot compel an internet service provider to produce information stored overseas. — Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016)," *Harvard Law Review*, vol. 130, pp. 769–776, 2016.
[38] "United States v Microsoft Corporation," No. 17-2; 584 U.S., 2018.
[39] (2018) Cloud security guidance: 2.1 physical location and legal jurisdiction. National Cyber Security Centre (UK). [Online]. Available: https://www.ncsc.gov.uk/collection/cloudsecurity/implementing-the-cloud-security-principles/asset-protection-and-resilience#physical

[40] C. Millard, “Forced localization of cloud services: Is privacy the real driver?” *IEEE Cloud Computing*, vol. 2, no. 2, pp. 10–14, 2015.
[41] A. Chander and U. P. Lê, “Data nationalism,” *Emory LJ*, vol. 64, pp. 677–739, 2014.
[42] A. Savelyev, “Russia’s new personal data localization regulations: A step forward or a self-imposed sanction?” *Computer Law & Security Review*, vol. 32, no. 1, pp. 128–145, 2016.
[43] S. Livingston and G. Greenleaf, “Data localisation in China and other APEC jurisdictions,” *Privacy Laws & Business International Report*, vol. 143, pp. 22–26, 2016.
[44] A. D. Mitchell and J. Hepburn, “Don’t fence me in: Reforming trade and investment law to better facilitate cross-border data transfer,” *Yale JL & Tech.*, vol. 19, pp. 182–237, 2017.
[45] “Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union,” *Official Journal of the European Union*, vol. L 303, pp. 59–68, 2018.
[46] S. D. Warren and L. D. Brandeis, “Right to privacy,” *Harvard Law Revue*, vol. 4, no. 5, pp. 193–220, 1890.
[47] “Universal Declaration of Human Rights,” United Nations, 1948.
[48] “Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights),” Council of Europe, 1950.
[49] “Charter of Fundamental Rights of the European Union,” *Official Journal of the European Union*, vol. C 303, pp. 1–16, 2007.
[50] “US Constitution, Amendment IV,” 1791.
[51] “Olmstead v. United States,” 277 U.S. 438, 1928.
[52] “Katz v United States,” 389 U.S. 347, 1967.
[53] “Halford v. The United Kingdom,” (20605/92) ([1997] 24 EHRR 523, 1997.
[54] (2019) Guide to international law and surveillance (2.0). Privacy International. [Online]. Available: https://privacyinternational.org/sites/default/files/2019-04/Guide%20to%20International%20Law%20and%20Surveillance%202.0.pdf
[55] Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, “Guiding principles on business and human rights: Implementing the united nations "protect, respect and remedy" framework,” United Nations, 2011.
[56] “Smith v Maryland,” 442 U.S. 735 (US S.Ct), 1979.
[57] A. M. Rutkowski, “International signals intelligence law: Provisions and history,” *Lawfare Research Paper Series*, vol. 42, pp. 933–988, 2017.
[58] N. Jupillat, “From the cuckoo’s egg to global surveillance: cyber espionage that becomes prohibited intervention,” *NCJ Int’l L.*, vol. 42, pp. 933–988, 2016.
[59] J. Hurwitz, “Encryption$^{\text{Congress}}$ mod (Apple+ CALEA),” *Harvard Journal of Law & Technology*, vol. 30, pp. 355–424, 2017.
[60] HIPCAR, “Interception of communications: Model policy guidelines & legislative texts,” International Telecommunications Union, 2012.
[61] “Council Resolution of 17 january 1995 on the lawful interception of telecommunications,” *Official Journal of the European Communities*, vol. C 329, pp. 1–6, 1995.
[62] (2019) Lawful Interception. ETSI. [Online]. Available: https://www.etsi.org/technologies/lawfulinterception
[63] L. Sacharoff, “Unlocking the fifth amendment: Passwords and encrypted devices,” *Fordham Law Revue*, vol. 87, pp. 203–251, 2018.
[64] M. J. Weber, “Warning-weak password: The courts’ indecipherable approach to encryption and the fifth amendment,” *University of Illinois Journal of Law*, pp. 455–486, 2016.
[65] “Investigatory Powers Act 2016,” United Kingdom, 2016.
[66] “Mapp v. Ohio,” 367 U.S. 643, 1961.
[67] (2014) R -v- coulson and others: Sentencing remarks of Mr Justice Saunders. [Online]. Available: https://www.judiciary.uk/wp-content/uploads/2014/07/

sentencing-remarks-mr-jsaunders-r-v-coulson-others.pdf
[68] "Handbook on European data protection law," European Union Agency for Fundamental Rights, 2018.
[69] (2019) GDPR: guidelines, recommendations, best practices. European Data Protection Board. [Online]. Available: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelinesrecommendations-best-practices_en
[70] R. Carolina. (2017) Why the EU has issued relatively few data protection adequacy determinations? a reply. Lawfare. [Online]. Available: https://www.lawfareblog.com/why-eu-has-issued-relatively-few-data-protection-adequacydeterminations-reply
[71] "Directive (EU) 2016/680 ... of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences..." *Official Journal of the European Union*, vol. L 119, pp. 89–131, 2016.
[72] (2018) D2.2: Review report on directive 2016/680 aimed at the judiciary. INtroduction of the data protection reFORM to the judicial system (INFORM). [Online]. Available: http://informproject.eu/wp-content/uploads/2018/05/D2.2.pdf
[73] (2018) D2.5 review report on directive (eu) 2016/680 aimed at the legal practitioners. INtroduction of the data protection reFORM to the judicial system (INFORM). [Online]. Available: http://informproject.eu/wp-content/uploads/2018/05/D2.5.pdf.
[74] "Breyer v Germany," Case C-582/14, 2016.
[75] "ISO/IEC 29100:2011 Information technology - Security techniques - Privacy framework," 2011.
[76] "Guide to Protecting the Confidentiality of Personally Identifiable Information," Special Publication 800-122, NIST, 2010.
[77] M. J. Wiebe, "Applying the video privacy protection act to modern technology [ellis v. cartoon network, inc., 803 f. 3d 1251 (11th cir. 2015)]," *Washburn Law Journal*, vol. 57, pp. 169–202, 2018.
[78] "In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 278 (3d Cir. 2016), cert denied, 137 S. Ct. 624 (2017)," 2017.
[79] "Eichenberger v. ESPN, Inc." 876 F.3d 979 (9th Cir. 2017), 2017.
[80] (2019) Guide to data protection. Information Commissioner's Office (UK). [Online]. Available: https://ico.org.uk/for-organisations/guide-to-data-protection
[81] The INFORM Project. [Online]. Available: http://informproject.eu
[82] "UK Data Protection Act 2018," United Kingdom, 2018.
[83] "Schrems v Data Protection Commissioner," Case C 362/14, ECLI:EU:C:2015:650, 2015.
[84] "Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679," European Data Protection Board, 2018.
[85] E. Preston and P. Turner, "The global rise of a duty to disclose information security breaches," *The John Marshall Journal of Information Technology & Privacy Law*, vol. 22, pp. 457–492, 2004.
[86] N. Robinson, V. Horvath, J. Cave, A. P. Roosendaal, and M. Klaver, "Data and security breaches and cyber-security strategies in the EU and its international counterparts," European Union, 2013.
[87] J. Joerling, "Data breach notification laws: An argument for a comprehensive federal law to protect consumer data," *Washington University Journal of Law & Policy*, vol. 32, pp. 467–488, 2010.
[88] "Wm Morrison Supermarkets PLC v Various Claimants," [2018] EWCA Civ 2339, 2018.
[89] (1990) Computer Misuse Act 1990. [Online]. Available: https://www.legislation.gov.uk/ukpga/1990/18/contents
[90] "Computer Fraud and Abuse Act," codified at 18 U.S.C §1030 et seq.
[91] (2001) Convention on cybercrime. European Treaty Series 185. Council of Europe. [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/

0900001680081561
[92] (2019) Chart of signatures and ratifications of Treaty 185. Council of Europe. [Online]. Available: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=x7nTJy1r
[93] "Computer Misuse Act 1990," United Kingdom, 1990.
[94] D. of Public Prosecutions (UK), "The Code for Crown Prosecutors," 2018.
[95] R. Carolina, "Legal aspects of software protection devices," *Computer Law and Security Report*, vol. 11, no. Jul-Aug, pp. 188–193, 1995.
[96] G. J. Edwards, "Self-help repossession of software: Should repossession be available in Article 2B of the UCC," *University of Pittsburgh Law Review*, vol. 58, pp. 763–788, 1997.
[97] N. Schmidle, "Digital Vigilantes," 7 May 2018, The New Yorker.
[98] S. Curry. Hack-back: Vigilantism in the connected world. Forbes, 7 January 2019. [Online]. Available: https://www.forbes.com/sites/samcurry/2019/01/07/hack-back-vigilantism-in-the-connected-world/#379ca3a55437
[99] (2019) Should companies risk going on the cyber offensive? Brink. [Online]. Available: http://www.brinknews.com/should-companies-risk-going-on-the-cyber-offensive/
[100] H. Beale, Ed., *Chitty on Contracts*, 33rd ed. Sweet & Maxwell, 2018.
[101] "Directive 2000/31/EC of the Eurpoean Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)," *Official Journal of the European Communities*, vol. L 178, pp. 1–16, 2000.
[102] "Fair and Accurate Credit Transactions Act of 2003," United States Statutes at Large, vol. 117, p. 1952, 2003.
[103] "Directive (EU) 2015/2366 Of The European Parliament And Of The Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 200," *Official Journal of the European Communities*, vol. L 337, pp. 35–127, 2015.
[104] "Uniform Commercial Code, Article 4A," The American Law Institute and the National Conference of Commissioners on Uniform State Laws.
[105] "Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)," *Official Journal of the European Communities*, vol. L 177, pp. 6–16, 2008.
[106] "Umpqua Bank, et al v Target Corp, (complaint)," MDL No. 14-2522 (PAM/JJK), Fed Dist Minnesota, (complaint filed Aug 1, 2014).
[107] "Dittman, et al v UPMC," No. 43 WAP 2017, 196 A.3d 1036 (Pa S.Ct), 2018.
[108] "The T.J. Hooper," 60 F.2d 737, 2d Cir, 1932.
[109] R. A. Epstein, "The path to "The TJ Hooper": the theory and history of custom in the law of tort," *The Journal of Legal Studies*, vol. 21, no. 1, pp. 1–38, 1992.
[110] "United States v. Caroll Towing," 159 F.2d 169, 2d Cir., 1947.
[111] P. J. Kelley, "The Carroll Towing Company case and the teaching of tort law," *Saint Louis University Law Journal*, vol. 45, pp. 731–758, 2001.
[112] "Restatement (Third) of Torts: Products Liability," American Law Institute, 1997.
[113] "Council Directive of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (85/374/EEC)," *Official Journal of the European Communities*, vol. L 210, pp. 29–33, 1985.
[114] "Evaluation of Council Directive 85/374/EEC of 25 July 1985 on the approximation of the liability for defective products," European Commission, 2018.
[115] "Liability for emerging digital technologies," SWD(2018) 137, European Commission, 2018.
[116] "Barnett v Chelsea & Kensington Hospital [1969]," 1 QB 428, 1969.
[117] "Dillon v. Twin State Gas & Elec. Co." 85 N.H. 449, New Hampshire, 1932.
[118] "Wagon Mound (No. 1) [1961] UKPC 2 ," Privy Council, 1961.

[119] "Hedley Byrne & Co Ltd v Heller & Partners Ltd," [1964] AC 465, 1963.
[120] "Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II)," *Official Journal of the European Union*, vol. L 199, pp. 40–49, 2007.
[121] "WIPO Copyright Treaty," World Intellectual Property Organization, Geneva, 1996.
[122] S. P. Calandrillo and E. M. Davison, "The dangers of the digital millennium copyright act: Much ado about nothing," *William and Mary Law Review*, vol. 50, pp. 349–415, 2008.
[123] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*. CRC press, 1997.
[124] G. Vetter, "Patenting cryptographic technology," *Chi.-Kent L. Rev.*, vol. 84, pp. 757–776, 2009.
[125] L. Khansa and C. W. Zobel, "Assessing innovations in cloud security," *Journal of Computer Information Systems*, vol. 54, no. 3, pp. 45–56, 2014.
[126] T. L. James, L. Khansa, D. F. Cook, O. Bruyaka, and K. B. Keeling, "Using network-based text analysis to analyze trends in microsoft's security innovations," *Computers & Security*, vol. 36, pp. 49–67, 2013.
[127] "Uniform Trade Secrets Act," Uniform Law Commission, National Conference of Commissioners on Uniform State Laws, 1985.
[128] J. H. Pooley, M. A. Lemley, and P. J. Toren, "Understanding the economic espionage act of 1996," *Tex. Intell. Prop. LJ*, vol. 5, pp. 177–229, 1996.
[129] "Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure," *Official Journal of the European Union*, vol. L 157, pp. 1–18, 2016.
[130] PricewaterhouseCoopers, "The scale and impact of industrial espionage and theft of trade secrets through cyber," European Commission, 2018.
[131] D. S. Levine and C. B. Seaman, "The DTSA at one: An empirical study of the first year of litigation under the defend trade secrets act," *Wake Forest L. Rev.*, vol. 53, pp. 105–156, 2018.
[132] J. Lane, "NTP, Inc. v. Research in Motion, Ltd.: Inventions Are Global, But Politics Are Still Local-An Examination of the BlackBerry Case," *Berkeley Tech. LJ*, vol. 21, pp. 59–77, 2006.
[133] P. Samuelson and S. Scotchmer, "The law and economics of reverse engineering," *Yale Law Journal*, vol. 111, pp. 1575–1663, 2002.
[134] P. J. Weiser, "The internet, innovation, and intellectual property policy," *Colum. L. Rev.*, vol. 103, pp. 534–613, 2003.
[135] P. Samuelson, "Anticircumvention rules: Threat to science," *Science*, vol. 293, no. 5537, pp. 2028–2031, 2001.
[136] C. Zieminski, "Game over for reverse engineering: How the DMCA and contracts have affected innovation," *Journal of Technology Law & Policy*, vol. 13, pp. 289–339, 2008.
[137] "Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs," *Official Journal of the European Union*, vol. L 111, pp. 16–22, 2009.
[138] P. Samuelson, "Freedom to tinker," *Theoretical Inquiries in Law*, vol. 17, no. 2, pp. 562–600, 2016.
[139] R. Verdult and F. D. Garcia, "Cryptanalysis of the megamos crypto automotive immobilizer," *USENIX; login*, vol. 40, no. 6, pp. 17–22, 2015.
[140] "Volkswagen Aktiengesellschaft vs Garcia, et al," [2013] EWHC 1832 (Ch), 2013.
[141] R. Carolina and K. G. Paterson. (2013) Megamos Crypto, Responsible Disclosure, and the Chilling Effect of Volkswagen Aktiengesellschaft vs Garcia, et al. [Online]. Available: http://www.origin.co.uk/download/43/
[142] R. Verdult, W. Meng, F. D. Garcia, D. Doozan, B. Ege, W. Enck, A. C. Snoeren, G. Vigna, T. Xie, N. Feamster *et al.*, "Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer," in *22nd {USENIX} Security Symposium ({USENIX} Security 13)*, 2013, pp. 687–702.

[143] "Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979)," 1979.
[144] "Prince plc v. Prince Sports Groups," [1998] F.S.R. 21, 1998.
[145] G. Sartor, "Providers Liability: From the eCommerce Directive to the Future," European Parliament, 2017.
[146] K. Perset, "The economic and social role of internet intermediaries," *OECD, Directorate for Science, Technology and Industry, OECD Digital Economy Papers*, 2010.
[147] T. Verbiest, G. Spindler, and G. M. Riccio. (2007) Study on the liability of internet intermediaries. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2575069
[148] "UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998," United Nations, 1999.
[149] A. M. Froomkin, "The essential role of trusted third parties in electronic commerce," *Oregon Law Review*, vol. 75, pp. 49–115, 1996.
[150] S. Mason, *Electronic signatures in law*, 4th ed. University of London, School of Advanced Study, Institute of Advanced Legal Studies, 2017.
[151] "Digital signature guidelines: Legal infrastructure for certification authorities and secure electronic commerce," American Bar Association, 1996.
[152] "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (Repealed)," *Official Journal of the European Union*, vol. L 13, pp. 12–20, 1999.
[153] "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," *Official Journal of the European Union*, vol. L 257, pp. 73–114, 2014.
[154] "Junger v Daley," 209 F.3d 481 (6th Cir.), 2000.
[155] J. R. Roig, "Decoding first amendment coverage of computer source code in the age of YouTube, Facebook, and the arab spring," *N.Y.U. Annual Survey of American Law*, vol. 68, pp. 319–395, 2012.
[156] D. W. Arner, J. Barberis, and R. P. Buckey, "Fintech, regtech, and the reconceptualization of financial regulation," *Northwestern Journal of International Law & Business*, vol. 37, pp. 371–414, 2017.
[157] "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," *Official Journal of the European Union*, vol. L 194, pp. 1–30, 2016.
[158] D. Thaw, "The efficacy of cybersecurity regulation," *Georgia State University Law Review*, vol. 30, pp. 287–374, 2014.
[159] "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification ... (Cybersecurity Act)," *Official Journal of the European Union*, vol. L 151, pp. 15–69, 2017.
[160] M. Libicki, "The coming of cyber espionage norms," in *2017 9th International Conference on Cyber Conflict (CyCon)*. IEEE, 2017, pp. 1–17.
[161] M. Dark, R. Epstein, L. Morales, T. Countermine, Q. Yuan, M. Ali, M. Rose, and N. Harter, "A framework for information security ethics education," in *10th Colloquium for Information Systems Security Education-University of Maryland*, vol. 4, 2006, pp. 109–115.
[162] ACM history. Association for Computing Machinery. [Online]. Available: https://www.acm.org/about-acm/acm-history
[163] "ACM code of ethics and professional conduct," Association for Computing Machinery, 2018.
[164] Using the code. Association for Computing Machinery. [Online]. Available: https://ethics.acm.org/code-of-ethics/using-the-code/
[165] (2019) Accredited companies - regions and services. Crest (International). [Online]. Available:

https://www.crest-approved.org/accredited-companies/index.html
[166] "CREST code of conduct for CREST qualified individuals (version 8.0)," Crest (GB) Ltd., 2016.
[167] A. M. Matwyshyn, A. Cui, A. D. Keromytis, and S. J. Stolfo, "Ethics in security vulnerability research," in *IEEE Security & Privacy*. IEEE Computer Society, March/April 2010, pp. 67–72.
[168] A. Maurushat, *Disclosure of security vulnerabilities: legal and ethical issues*. Springer, 2013.
[169] (2018) The Equities Process. National Cyber Security Centre (UK). [Online]. Available: https://www.gchq.gov.uk/information/equities-process
[170] (2019) Responsible release principles for cyber security vulnerabilities. Australian Signals Directorate. [Online]. Available: https://www.asd.gov.au/publications/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities.pdf
[171] (2019) Vulnerabilities equities process. Electronic Privacy Information Center. [Online]. Available: https://epic.org/privacy/cybersecurity/vep/
[172] (2019) EFF v. NSA, ODNI - Vulnerabilities FOIA. Electronic Frontier Foundation. [Online]. Available: https://www.eff.org/cases/eff-v-nsa-odni-vulnerabilities-foia
[173] N. Asokan, "Ethics in information security," in *IEEE Security & Privacy*. IEEE Computer Society, 2017.
[174] M. Goldstein, A. Stevenson, and L. Picker, "Hedge Fund and Cybersecurity Firm Team Up to Short-Sell Device Maker," The New York Times, 8 September 2016.
[175] "ISO/IEC 29147:2014 Information Technology - Security techniques - Vulnerability dislcosures," 2014.
[176] "ISO/IEC 30111:2013 Information technology - Security techniques - Vulnerability handling processes," 2013.
[177] "Coordinated vulnerability disclosure: the guideline," National Cyber Security Centre (NL), 2018.
[178] (2018) NCSC vulnerability disclosure co-ordination. National Cyber Security Centre (UK). [Online]. Available: https://www.ncsc.gov.uk/blog-post/ncsc-vulnerability-disclosure-co-ordination
[179] D. Feldman, "The nature of legal scholarship," *Modern Law Review*, vol. 52, pp. 498–517, 1989.
[180] G. A. Spann, "Baby M and the Cassandra problem," *Georgetown Law Journal*, vol. 76, pp. 1719–1739, 1987.
[181] K. Takayanagi, "Contact of the common law with the civil law in japan," *The American Journal of Comparative Law*, vol. 4, pp. 60–69, 1955.
[182] C. Reed and A. Murray, "Rethinking the jurisprudence of cyberspace," 2018.
[183] D. Gerard, *Attack of the 50 foot blockchain: Bitcoin, blockchain, Ethereum & smart contracts*. David Gerard, 2017.
[184] "Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters," *Official Journal of the European Union*, vol. L 351, pp. 1–32, 2012.
[185] L. Kasdan, Director, "Silverado," FILM, Columbia Pictures, 1985.
[186] A. M. Froomkin, "Wrong turn in cyberspace: Using ICANN to route around the APA and the Constitution," *Duke Law Journal*, vol. 50, pp. 17–184, 2000.
[187] (2019) URL List. Internet Watch Foundation. [Online]. Available: https://www.iwf.org.uk/become-a-member/services-for-members/url-list
[188] P. Mell, T. Grance *et al.*, "The NIST definition of cloud computing," NIST, 2011.
[189] "Explanations relating to the charter of fundamental rights," *Official Journal of the European Union*, vol. C 303, pp. 17–35, 2007.
[190] "Carpenter v US," 138 S.Ct. 2206, 585 U.S., 2018.
[191] (2016) Canary watch – one year later. Electronic Frontier Foundation. [Online]. Available: https://www.eff.org/deeplinks/2016/05/canary-watch-one-year-later
[192] "Brady v. Maryland," 373 U.S. 83, 1963.
[193] "R v Gold and Schifreen," [1988] AC 1063, [1988] Crim LR 437 (HL), 1988.
[194] B. Sterling, *The hacker crackdown: Law and disorder on the electronic frontier*. Bantam Books

New York, 1992, vol. 1.
[195] C. Stoll, *The cuckoo's egg: tracking a spy through the maze of computer espionage*. Doubleday, 1989.
[196] M. Perrow. (2009) Click's botnet experiment. [Online]. Available: https://www.bbc.co.uk/blogs/theeditors/2009/03/click_botnet_experiment.html
[197] R. Carolina. (2009) Opinion: BBC Click exploited world's poor and vulnerable. [Online]. Available: https://www.computerweekly.com/opinion/Opinion-BBC-Click-exploited-worlds-poor-and-vulnerable
[198] ——. (2009) Opinion: The unanticipated consequences of BBC Click's botnet crime. [Online]. Available: https://www.computerweekly.com/opinion/Opinion-The-unanticipated-consequences-of-BBC-Clicks-botnet-crime
[199] (2009) BBC team exposes cyber crime risk. BBC. [Online]. Available: http://news.bbc.co.uk/1/hi/programmes/click_online/7932816.stm
[200] D. Etcovitch and T. van der Merwe, "Coming in from the Cold: A Safe Harbor from the CFAA and the DMCA §1201 for Security Researchers," Research Publication No. 2018-4, Berkman Klein Center, 2018.
[201] "Palsgraf v. Long Island Railroad Co." 248 N.Y. 339, 162 N.E. 99, N.Y Ct of Appeals, 1928.
[202] "Cooney v Chicago Public Schools," 943 N.E.2d 23 (Illinois Appellate Ct, 1st District, 2010), appeal denied 949 N.E.2d 657 (S.Ct Illinois, 2011), 2010.
[203] S. Pettypiece and E. Dexheimer, "Target Reaches $67 Million Agreement With Visa Over Breach," Bloomberg, 18 August 2015.
[204] J. Stempel and N. Bose, "Target in $39.4 million settlement with banks over data breach," Reuters, 3 December 2015.
[205] F. Rosselli, "Analysis of the economic impact of the development risk clause as provided by Directive 85/374/EEC on liability for defective products," Ares(2014)3310430 - 07/10/2014, European Commission, 2014.
[206] F. D. Prager, "The influence of Mr. Justice Story on american patent law," *The American Journal of Legal History*, vol. 5, pp. 254–264, 1961.
[207] "Ungar v Sugg," (1892) 9 RPC 113, 1892.
[208] C. Yang. (2005) The BlackBerry Widow's Tale. [Online]. Available: https://www.bloomberg.com/news/articles/2005-12-18/the-blackberry-widows-tale
[209] P. Samuelson, "Intellectual property and the digital economy: Why the anti-circumvention regulations need to be revised," *Berkley Technology Law Journal*, vol. 14, pp. 519–566, 1999.
[210] "Haberman v Jackel International," [1999] FSR 683, 1999.
[211] (2019) Woodhull freedom foundation et al. v. united states. Electronic Frontier Foundation. [Online]. Available: https://www.eff.org/cases/woodhull-freedom-foundation-et-al-v-united-states
[212] R. Romano. (2019) A new law intended to curb sex trafficking threatens the future of the internet as we know it. [Online]. Available: https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom
[213] J. E. Cohen, "The zombie First Amendment," *William and Mary Law Review*, vol. 56, pp. 1119–1158, 2015.
[214] B. Lee, "Where Gutenberg meets guns: The liberator, 3d-printed weapons, and the First Amendment," *NCL Rev.*, vol. 92, pp. 1393–1425, 2014.
[215] E. T. Jensen, "The Tallinn Manual 2.0: Highlights and insights," *Georgetown Journal of International Law*, vol. 48, pp. 735–778, 2016.
[216] J. Markoff, "Apple's Engineers, if Defiant, Would be in Sync With Ethics Code," The New York Times, 18 March 2016.

ACRONYMS

ccTLD Country Code Top-Level Domain. 12

DES Data Encryption Standard. 47

EEA European Economic Area. 15, 24, 25

ETSI European Telecommunications Standards Institute. 17

GDPR General Data Protection Regulation. 11, 12, 20, 22, 23, 25–27, 74

IGO International Governmental Organisation. 24

IMAP Internet Mail Access Protocol. 19, 32, 69

LAN Local Area Network. 9, 19, 30

PCI-DSS Payment Card Industry Data Security Standard. 33

PII Personally Identifiable Information. 20, 21

PSTN Public Switched Telephone Network. 18

RSA Rivest, Shamir, and Adelman public key encryption. 47

SaaS Software as a Service. 22, 41

SWIFT Society for Worldwide Interbank Financial Telecommunication. 14, 15, 70

TLD Top-level Domain. 12

WAN Wide Area Network. 30

GLOSSARY

consumer In the context of a given transaction, a natural person who enters into a transaction other than for business or professional purposes. A given person may act as a consumer in some transactional contexts, and a non-consumer in others. N.B. This definition is far from universal. Some laws in some states adopt definitions of 'consumer' that vary from this. 34, 35, 37, 52, 54–56, 71, 73

cyberspace A global domain within the information environment consisting of an interdependent network of information system infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Source: NISTIR 7298 (rev2). 3, 6, 9, 17, 27, 29, 31, 41, 55, 63, 66

international governmental organisation A legal person established and recognised as such by more than one state pursuant to treaty (e.g., the United Nations, INTERPOL, the International Maritime Organization, etc.). In practice, often simplified as 'International Organisation' or 'Treaty Organisation'. 24, 56, 59, 67

jurisdiction See the discussion in Section 2. 4–6, 9–15, 18, 20, 26, 35, 36, 43, 44, 55, 56, 63, 66–69, 71, 74

legal action The process by whereby a person brings a legal claim to a tribunal for adjudication or to enforce the results of a prior adjudication. 7, 9, 10, 13, 19, 32, 36, 37, 40–43, 45–50, 55, 57, 60, 64, 69, 71, 73

legal person An entity vested with sufficient characteristics of personhood to merit a legal identity separate from its constituent members. These characteristics include: the right to commence or respond to legal action in the entity's name; the right to own assets in the entity's name; and the right to enter into obligations in the entity's name. Legal persons generally include: states; international governmental organisations; public or private entities incorporated pursuant to the law of a state and vested by that state with the characteristics of personhood, such as an English public limited company (PLC), a Delaware limited liability partnership (LLP), a French société anonyme (S.A.), a German gesellschaft mit beschränkter hafting (GmbH), the City of New York, etc.. 11, 20, 64, 67

natural person A human being, living or deceased. 13, 20, 22, 25, 26, 42, 64

person A natural person or legal person. 3, 7, 9–15, 28–31, 33, 36, 45–49, 53–55, 57, 58, 63, 67, 70, 73

proof (prove) See the discussion in Section 1.3. 4, 6, 7, 9, 46, 48, 64, 66, 67, 70

right of action A right arising in law for one person to take legal action against another. 41

state A legal person that normally possesses the following qualifications: a permanent population; a defined territory; a government; and a legal capacity to enter into relations with other states. In the context of pubic international law and diplomacy, confirming the status of an entity as a 'state' is a decision normally made individually by other states through proclamation, exchange of ambassadors, etc. In the context of a federation (e.g., States of the US, States of Australia, Provinces of Canada, Länder of Germany), recognition normally takes place in accordance with the constitutional procedures of that federation.. 3–20, 23–31, 34, 36, 40, 42–44, 60, 64, 66–70

territory (territorial, territoriality) A delimited region of geographic space (i.e., real space, including air and water). Often used in law to describe boundaries of a state (e.g., the territory of the Republic of Italy). 9–15, 18, 51, 57–59, 66–68, 72–74