Managing the hypercomplexity of cyber security regulation: In search of a regulatory Rosetta Stone

Received (in revised form): 11th May, 2019

F. Paul Greene
Partner, Privacy & Data Security Practice Group Leader, Harter Secrest & Emery

F. Paul Greene is a partner and the Privacy & Data Security Practice Group Leader at Harter Secrest & Emery LLP. Paul represents clients in a wide range of industries concerning all aspects of proactive preparation and risk management, including security and vulnerability assessments, policy and procedure review, breach response planning and drills, as well as board and management education on cyber risk and privacy issues. Post-breach, Paul and his team provide a full array of reactive services, including breach coaching and response, crisis management and communication, internal and governmental investigations, breach notification and potential litigation or regulatory action including under the EU's General Data Protection Regulation (GDPR), the Personal Information Protection and Electronic Documents Act (PIPEDA) and the upcoming California Consumer Privacy Act (CCPA). Paul is a Certified Information Privacy Professional/ United States (CIPP/US) recognised by the International Association of Privacy Professionals (IAPP) and is a Distinguished Fellow of the Ponemon Institute. He has also been recognised by Chambers USA: America's Leading Lawyers in Business since 2015 for his strong reputation and knowledge, especially in the field of complex commercial litigation. He publishes and speaks internationally on privacy and information security issues and is an adjunct professor at the Rochester Institute of Technology, teaching information security policy and law to computer science and cyber security students, both on the graduate and undergraduate levels. Paul received his JD from Fordham University, his PhD from New York University and his BA from the University of Rochester.

Harter Secrest & Emery LLP, Attorneys and Counselors, 1600 Bausch & Lomb Place, Rochester, NY 14604-2711, USA
Tel: +1 585-231-1435; E-mail: FGreene@hselaw.com

Abstract It is an understatement to say that the legal issues arising from privacy and information security concerns are complex. Indeed, the way that laws from various jurisdictions and industry sectors interact and even conflict make the legal issues in this space hypercomplex: more complex because of their very own complexity. Fortunately, a common regulatory language is beginning to coalesce, and organisations can position themselves within this 'sweet spot' of regulatory focus. By engaging in robust and honest risk assessments, by adopting an established security framework, and by including regulatory risk in its risk management and budgeting efforts, an organisation can adapt to the changing regulatory landscape and lessen the burden that this hypercomplexity creates.

KEYWORDS: cyber security, privacy, GDPR, CCPA, HIPAA, risk assessment, NIST

INTRODUCTION

Data is ubiquitous, and its volume is increasing at an exponential rate. Data is also not static: by its very nature, it wants to and will invariably move. Yet the movement of data — transfer from one medium to another, or from one user to another — is anathema to conventional conceptions of information security, most certainly to how information security has been conceived of under law.[1] According to this conception, information security is, in the end, a discipline aimed at restricting the movement of data across systems, networks,

or among users. Put simply, under current legal conceptions of information security, less movement equals more security.[2]

Against this backdrop, jurisdictions around the globe have been struggling for over two decades with how best to induce more controlled movement of sensitive data, in an ultimate effort to combat the rise of Internet-enabled crime. As is well known in the US, however, there has been little uniformity in how jurisdictions have approached this goal. Some of the basic questions posed have been these: should legislatures mandate specific rules to restrict unauthorised movement of data, or should best practices be left to industry organisations to develop? Should legal information security rules be prescriptive, giving clarity as to what is expected under the law, or risk-adjusted, allowing entities to scale their security efforts to the risks they perceive? Or should the rules grow out of a common-law or quasi-common-law framework, built upon decisional law or administrative settlements, such as those involving the US Federal Trade Commission (FTC)? Should these rules be top-down, coming from either national jurisdictions or international groups of jurisdictions, or bottom-up, coming from municipalities, provinces or states? There are as many answers to these questions as the questions themselves, leading to the current state of hypercomplexity in relation to information security regulation globally.

WHY HYPERCOMPLEXITY?

Simple complexity exists in the sheer number of jurisdictions that can potentially come into play, numbering over 50 in the US alone. Hypercomplexity arises when these overlapping systems of regulation interact and affect each other, becoming more complex by way of the system's own complexity. For example, when these regulatory schemes strive to determine what information security practices may be 'reasonable' under the circumstances,[3] confusion often ensues. In the US, for example, many regulatory schemes require a covered organisation to engage in defined, or sometimes undefined, 'reasonable' cyber security efforts. This requirement can be codified into law, such as in the recently amended Delaware breach notification law, or implied by law, such as in the FTC's fluid approach to information security regulation under the Federal Trade Commission Act.[4] Yet what is considered reasonable in one regulated sector can be easily influenced by what is required in another.[5] It is difficult to argue, for example, that encryption of healthcare data is truly only 'addressable', ie optional under certain circumstances, when applying the US Health Insurance Portability and Accountability Act of 1996 (HIPAA), when encryption of the same exact data can be required unless 'infeasible' under the Cybersecurity Requirements for Financial Services Companies promulgated by the New York State Department of Financial Services at 23 NYCRR Part 500 (Part 500).[6]

Given this interconnected and fluid system of regulation, any one data element on any one system can be subject to dozens of differing, and sometimes conflicting, information security requirements under relevant statute and regulation. Yet those who actually do information security, ie chief information security officer (CISO) and security engineers, are generally not trained in analysing laws and regulations, leaving us with systems and organisations that may exhibit substantively good information security practices, but nonetheless may be out of compliance with relevant legal mandates.

This disconnect between substantive security and legal compliance creates risk. In relation to an information security incident, immediate incident response, remediation and recovery can be the least of an organisation's worries. The legal and regulatory aftermath that follows, ranging from reporting to governmental agencies and affected individuals to regulatory action and class action lawsuits, often poses far greater cost and disruption to the organisation than

the incident itself. For example, a 7 Bitcoin SamSam ransom paid by a hospital to release encrypted medical records can be dwarfed by the cost and disruption caused by forensics, breach notification, regulatory investigation and potential fines that can follow.

It is no surprise, then, that security professionals have identified the increase in compliance-related activities as one of the key obstacles to proper threat detection and response. A recent study from the Ponemon Institute explored the risk created by 'resident' or 'post-breach' attacks, ie attacks that occur from inside the network perimeter. The study asked respondents to identify the four biggest '[o]bstacles to an organization's ability to detect cyberattackers within [a] network'. Sixty per cent of the responses identified 'compliance activity' as a top-four risk that 'detracts attention from threat detection functions'. This was the highest response percentage for this question, with 11 separate response options given.[7] The lowest percentage-specific response, at 15 per cent, was that '[e]ffective detection technologies are not available in the marketplace', indicating that although technology may be up to the task of thwarting attacks, legal compliance may often get in the way.[8]

What is missing in all of this — if such a thing is at all possible — is a unified approach to compliance with the various legal mandates that can apply to an organisation's information security efforts. To everyone's detriment, no regulatory 'Rosetta Stone' yet exists to translate between applicable legal schemes, creating a unified language for use with regulators, legislators, courts, law enforcement and the public in relation to information security. This, of course, creates further risk, as compliance with these competing and overlapping regulatory schemes will often be in the eye of the beholder. Post-incident, hindsight in relation to information security is usually negative and 20/20, highlighting flaws in an organisation's information security programme that may not have presented as flaws before the incident. In the end, a system is secure only until it is not, and a security incident often proves the existence of a flaw or vulnerability that may not have been perceivable before.

This paper outlines the primary challenges caused by the proliferation of cyber security regulation globally over the last decade, and offers strategies for managing what has become a hypercomplex, increasingly fluid and undefined area of the law. The term 'undefined' may seem out of place in relation to a proliferation of codified security rules, but between the written lines of such rules, grey areas and gaps abound, allowing for or requiring regulatory guidance and human interpretation of the written legal and regulatory texts, creating even more complexity. In the end, only a unified standard of base-line cyber security requirements, akin to the Uniform Commercial Code in relation to the sale of goods in the US, or the UN Convention on the International Sale of Goods internationally, will have the ability cure this complexity. The trend, however, has been for less uniformity in this space rather than more, and no such universal convention for cyber security regulation is on the international legal horizon.[9]

SOURCES OF COMPLEXITY IN CYBER SECURITY REGULATION

When it comes to regulating cyber security,[10] there are as many approaches as there are jurisdictions in question. States (in the international sense) as well as individual states, provinces and even localities have entered the fray, creating rules either out of whole cloth, or in reaction to, or in emulation of, other, neighbouring jurisdictions that have adopted cyber security rules. This has led to a crazy quilt of overlapping, intermeshing and often conflicting rules and requirements that entities of all sizes must address when

processing personal information — case in point, the 50 states in the US, together with three territories and the District of Columbia (the constitutionally created, non-state jurisdiction encompassing Washington, DC), which have all adopted their own data breach notification laws. Rarely do an organisation's activities stop at a state line, however, and most certainly not in relation to the processing of personal information. This requires many, if not most, US entities to undertake a detailed analysis of what types of personal information they collect and where the relevant data subjects reside. And because a growing number of state data breach notification laws purport to reach beyond their states' borders, encompassing any person or entity anywhere that processes personal information concerning a resident of one of those states, even a purely local establishment is potentially subject to laws made hundreds or thousands of miles away.[11]

For national, international or global organisations, the complexity increases, such that dozens of differing information security laws could apply to the same operations vertical, eg the organisation's human resources function or its marketing function. For an example of how these laws can differ, one need only look back to the individual states in the US. To begin with, a defined and reportable breach in one state may not be a breach in another. In certain states, reporting duties are triggered by unauthorised access to or acquisition of defined personal information, while in other states, a harm threshold must be met, such as a 'reasonabl[e] likel[ihood] to cause substantial harm to the individuals to whom the information relates', before a reporting duty is triggered.[12] This leads to an often complex and tortuous decision tree for a breached entity: whether to report a breach not only in a state where that state's breach notification law has been triggered, eg Georgia because there was unauthorised acquisition, but also in a neighbouring state where the breach notification law was not triggered, eg Alabama because there was no reasonable likelihood of substantial harm.[13] The organisation may have, for example, employees or customers in both states, and it can be difficult to explain to customer X why the customer did not receive notice of a nationwide breach, while customer Y from a neighbouring state did.

Add to this the fact that US state attorneys general often work together on multi-state breaches, then compliance with the letter of the law becomes the threshold question, with considerations such as public relations, regulator expectations and risk management playing an equal if not greater role.[14] In this regard, balancing the overlapping and often conflicting laws that may apply to a security incident becomes more art than science, which can be a common phenomenon in the representation of highly regulated entities. For such highly regulated entities, especially in the cyber security space, a well-informed entity knows what is expected under the law, whereas a better-informed one knows what is specifically expected by the regulator. Yet the snag with cyber security regulations is that they touch effectively all organisations that process personal data, not just those in historically highly regulated industries such as banking or healthcare, and many organisations have yet to learn which cyber security regulators have jurisdiction over them.

Case in point, the General Data Protection Regulation (GDPR) in the European Union (EU), which extends its territorial scope to entities that process personal data: (i) 'in the context of any establishment of a controller or processor in the Union, whether the processing takes place in the Union or not'; or in relation to either (ii) 'the offering of goods or services, irrespective of whether payment of the data subject is required, to such data subjects in the Union'; or (iii) 'the monitoring of their behaviour as far as their behaviour takes place within the Union'.[15] For entities outside the EU, this three-part test is fluid. Each prong

of the test involves a facts and circumstances analysis, even 'establishment', which includes 'the effective and real exercise of activity through stable arrangements … [with t]he legal form of such arrangements [not being] the determining factor in that respect'.[16] The interpretation of 'establishment' thus changes according to the circumstances, with EU courts finding establishment, for example, where a company organised outside of the Union utilised a language of a Member State (there, Hungary) and offered services in relation to real estate within that Member State.[17] Further, as famously held in the *Google Spain* case, a non-EU entity with an EU subsidiary can be found to be established in the EU, even if the operations of the subsidiary do not directly relate to the rights at issue, there the right to be forgotten.[18] Hence, under EU law, 'establishment' may only be conclusively determined once a court of competent jurisdiction examines the question. There is no uniform and conclusive listing of all entities 'established' in the EU for purposes of determining territorial scope under the GDPR.[19]

Which begs the question, how well does a legal framework function in relation to cyber security when you need sophisticated legal counsel to decipher it? Most organisations do not have the in-house legal capacity to properly parse and apply applicable cyber security law to the organisation's operations, let alone established outside legal relationships with such experience. Rather, many organisations rely on their information technology function — if they have one — or their cyber security function — if they are of the limited subset of entities that have such a function in house — to understand how law and cyber security intersect. But just as an organisation should not get its substantive cyber security advice from a lawyer, an organisation is ill-served if it is getting its legal advice from a cyber security professional. In today's highly regulated cyber security landscape, both functions are vital: cyber security to develop, implement, monitor and adjust an organisation's information security programme; and legal to help the organisation chart its course through the hypercomplex and changing regulatory landscape.

Adding to this challenge is the fact that with this complexity comes a wave of misinformation. Non-legal vendors of all stripes supply what appears to be legal advice concerning privacy-related and security-related regulatory schemes such as HIPAA, the GDPR and Part 500. Much of this advice is geared, however, at selling the vendors' services, where accuracy is often sacrificed for effect. Case in point, the myriad industry updates that circulated prior to the 25th May, 2018 implementation date of the GDPR, which ignored the complexity of the Article 3 territorial scope analysis outlined above, claiming instead that the GDPR applied to all entities processing personal data of EU citizens, regardless of the circumstances.[20] Further case in point, HIPAA, where vendors regularly assert that HIPAA applies to the processing of healthcare data, regardless of the circumstances. HIPAA, however, limits its application to healthcare providers that transmit electronic data in relation to certain transactions, health plans, healthcare clearing houses (together 'covered entities'), as well as defined business associates to these covered entities. A fitness device developer that collects user health-related data in the cloud, for example, is not — without more — a HIPAA covered entity.

Hence, the sources of complexity in this space include not only the numerous jurisdictions that have created substantive rules concerning the security and confidentiality of personal data, but also the regulators that enforce the rules, the grey areas concerning rule scope, the lack of legal training among information security professionals, the changing nature of the regulated entities themselves, as well as the misinformation that abounds in relation to the rules that apply. Each of these sources

interacts with and affects the others, resulting in a hypercomplex compliance dynamic that can be impossible to master.

SPECIAL CONSIDERATIONS IN RELATION TO EXTRATERRITORIAL REACH

Perhaps the greatest challenge posed by developing bodies of cyber security law and regulation in the past decade has been the rise of extraterritorial reach. In the early years of cyber security regulation, jurisdictions would generally limit applicability of their cyber security rules to the geographic boundaries of the jurisdiction in question. The initial US efforts at sectoral regulation of cyber security, such as HIPAA and Gramm-Leach-Bliley Act (GBLA), were of primary effect in the US. Certain international entities may have been regulated at the fringes of these schemes, for example in their roles as third-party service providers. But because the approach was sectoral, eg focused on the US healthcare or financial services industries, the reach of these laws was often geographically limited.

That began to change when jurisdictions shifted their focus from sectoral regulation to data-driven regulation, following the data in question, instead of a specific industry or sector. For example, HIPAA's original threshold question in relation to its territorial reach was whether an organisation was a defined covered entity. That threshold question expanded significantly in the HITECH amendments to HIPAA in 2009, which created first-person compliance obligations for any defined service provider to a covered entity, termed a business associate.

A similar, purely data-driven approach is found in Massachusetts, under 201 CMR 17.00 and Nevada, under Nev. Rev. Stat. Chap. 603A. The threshold question under the Massachusetts law is not what kind of organisation has the data, but what kind of data the organisation has. If the organisation possesses 'personal information about a resident of the Commonwealth, then the organisation must comply with the requirements of § 17.00'.[21] The same holds true for Nevada, which extends its reach to 'any governmental agency, institution of higher education, corporation, financial institution or retail operator or any other type of business entity or association [regardless of geography] that, for any purpose, whether by automated collection or otherwise, handles, collects, disseminates or otherwise deals with nonpublic personal information'.[22]

A permutation of this is the global effect felt by regulatory efforts of smaller jurisdictions. As noted above, the small US state of Delaware — which has just under 1m residents[23] and is less than one-fifth the size of Belgium — requires companies that do business within the state to engage in undefined 'reasonable' cyber security practices in relation to the personal data those entities collect, store and otherwise process. At first blush, this would seem to be of little importance on the world regulatory stage, but many of the largest corporations in the US are incorporated in Delaware, because of that state's favourable business laws and courts. Further, New York State, in promulgating Part 500 effective 1st March, 2017, extended its cyber security reach worldwide to cover any person or entity 'operating under or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the [New York] Banking Law, the Insurance Law, or the Financial Services Law'. This has swept organisations into the Part 500 net located in all 50 states as well as Canada, Japan, England, France and elsewhere.[24] And as jurisdictions begin to focus on the third parties that provide services to the entities directly covered by cyber security regulatory schemes, whether they be business associates under HIPAA, Third Party Service Providers under Part 500 or Processors under the GDPR, this extraterritorial expansion of security-related

and privacy-related requirements will only increase.

THE SPEED OF CHANGE

Not only have cyber security rules proliferated globally over the last decade, the proliferation is accelerating. The year 2018 alone saw changes in at least ten US states in relation to data breach notification and cyber security requirements, the GDPR coming into force, other cyber security and privacy laws advancing around the world, such as the Brazilian General Data Protection Law, passage of the California Consumer Privacy Act, which contains a private right of action arising from security breaches,[25] and mandatory breach notification requirements in Canada, with potential global effect.

This speed of change has two primary drivers: the crisis mentality surrounding privacy and cyber security concerns generally; and the shift away from purely legislative responses to that crisis. The California Consumer Privacy Act, for example, was passed in an effort to stave off a potentially more onerous and expansive ballot initiative promoted by a wealthy privacy advocate. In response to the initiative, the California legislature proposed, debated and passed the over 10,000-word Act in seven days,[26] a lightning-fast reaction that has led to what some have identified as problems in the law.[27] In New York — in response to the 2017 Equifax breach — the New York State Department of Financial Services, within nine business days after public announcement of the breach, proposed and then ultimately adopted revisions to its regulations to bring consumer credit reporting agencies such as Equifax under the jurisdiction of the department, including in relation to the cyber security requirements of Part 500.[28]

Speed of change, however, is deadly when it comes to developing a well-informed culture of compliance within an organisation. Organisations follow the rules best when those rules are well understood and static. Yearly or monthly changes in applicable regulatory frameworks require a nimbleness in the compliance function that few organisations can muster.

MANAGING THE HYPERCOMPLEXITY

Three primary strategies can help in addressing this fluid compliance landscape: embracing change; adopting a framework; and planning for regulatory risk.

Embracing change means recognising that, in relation to cyber security and privacy regulation, we — on a global scale — remain in flux. It means that the most important step in creating a comprehensive information security programme is undertaking a full and frank risk assessment, which allows the organisation to assess both information security risk and regulatory risk in real time, categorising those risks in relation to both likelihood of occurrence and severity of impact. Why regulatory risk? If an organisation assesses only substantive security risk in its periodic risk assessment, it is considering only half of the risk equation. For some, such as healthcare and financial services institutions, regulatory risk is existential; without demonstrable compliance with applicable requirements, the organisation can potentially lose its charter or licence or be subject to an investigation that destroys its reputation. For others, regulatory risk will be lower, but never non-existent. In 2016, the US Federal Trade Commission announced that 70 per cent of its cyber security-related investigations ended with a finding of no fault.[29] This was cold comfort to the organisations that had endured the cost and disruption of an FTC investigation, only to learn in the end that the FTC agreed with their approach to cyber security generally.

How can an organisation embrace this level of change as a practical matter? By increasing the frequency with which it assesses risk and its resulting approach to

information security. Most regulatory frameworks that require a risk assessment do not define the frequency in which risk assessments must be repeated. That can lead to an organisation choosing a longer period between risk assessments over a shorter one, in order to reduce cost or organisational disruption, for example. The added cost of an annual over biannual risk assessment, however, can be easily outweighed by the nimbleness and flexibility gained via more frequent review of security risks, regulatory risks and resulting controls. For example, a risk assessment conducted today but only repeated every two or three years would miss the regulatory risk created by the California Consumer Privacy Act, which comes into force next year and — as currently drafted — would allow for a private right of action in relation to certain security failings. And by increasing the frequency of risk assessments, the likelihood increases that security controls will change over time, leading to a less static, more dynamic approach to security generally. If an organisation becomes accustomed to security change, it will build muscle memory to deal with inevitable regulatory change.

Adopting a framework means not creating ad hoc solutions to regulatory requirements. By using an established security framework, an organisation helps create a narrative that can show appropriate cyber security efforts across a number of regulatory schemes. Indeed, in this regard, much of the necessary translation work has already been done. Cyber security professionals have already created crosswalk comparisons of substantive security frameworks, amounting to a kind of 'Rosetta Stone' for substantive security.[30] Certain regulatory schemes have also adopted — whether tacitly or expressly — established cyber security frameworks into their substantive rules. Specifically, Part 500 follows much of the structure of the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), and the US Department of Health and Human Services has also supported a NIST-based approach.[31] Readily available resources crosswalk NIST requirements to other security frameworks,[32] putting us but one step removed from a common regulatory language in relation to security, at least in certain sectors. And more light is on the horizon as jurisdictions begin to recognise substantive security frameworks as sufficient under the circumstances to show legal compliance. For example, the GDPR allows for the endorsement of security standards,[33] and a recently passed law in Ohio creates an affirmative defence to private tort causes of action arising from a data breach if the breached entity can show that it applied any one of a number of generally accepted security frameworks, including ISO 27001, NIST CSF or the Center for Internet Security Critical Controls.[34] Of course, further development in this vein will help lessen the hypercomplexity organisations currently face in relation to privacy and cyber security regulation.

When it comes to the choice of a specific framework, however, that decision can depend on the organisation, its industry, its resources and the risks it faces. The NIST framework generally, as expressed in NIST Special Publication 800-53 and related publications, has become a kind of lingua franca in certain sectors in the US, with the US Government using its purchasing power to require certain federal suppliers and even higher education institutions to adopt a NIST-based approach. For those outside of the federal marketplace, and perhaps with fewer resources, the NIST CSF provides a scaled-down, but nonetheless effective, version of the NIST approach, and has been sanctioned, for example, in a number of industries, including by regulators in the financial services and healthcare spaces. For international organisations, an ISO approach may be more appropriate, given the fact that a NIST-based approach has primarily been adopted in the US. Regardless of which framework may be most appropriate, framework choice must

be driven by two primary concerns: how well will the framework help improve my organisation's substantive security posture; and how well will it allow my organisation to justify that posture to a regulator, court, the general public or internally within the organisation.

Lastly, planning for regulatory risk means realising that compliance is never perfect, but the risk that arises from non-compliance is a business risk that can be managed. Risk transfer vehicles such as contractual indemnification and cyber risk insurance can help address the lack of certainty created by regulatory proliferation. Proper budgeting for incident response and regulatory inquiries is another useful tool. Indeed, the New York Department of Financial Services has recognised this, asking certain entities covered under Part 500 in their annual examinations whether they have budgeted for incident response. Of course, many entities are still at the planning stage when it comes to incident response, as they strive to develop an executable, well-understood incident response plan. Proper budgeting for incident response, as well as preparing for organisational disruption arising from compliance and reporting activities, is the logical next step.

CONCLUSION

An arms race is under way in the field of cyber security and privacy regulation, with competing jurisdictions emulating and often outdoing each other when it comes to protecting covered systems and data. Unfortunately, the victims of this arms race are often the organisations subject to regulation, which face frequent change and substantial uncertainty when adapting to new rules to even newer technologies and products. Although perfect translation between and among the often competing regulatory schemes is still elusive, organisations can take steps to manage the complexity that they face, specifically by embracing change, adopting established frameworks and planning for regulatory risk. Some regulatory risk will remain irreducible, but without proper management, regulatory risk can often outstrip the risk of a security breach itself.

References and notes

1. Less conventional conceptions of information security, such as the use of distributed ledger technology to ensure the confidentiality and integrity of data, focus instead on transparency rather than pure restriction of movement. Such a conception has yet to be adopted under law, however, eg ensuring security by mandating transparency and distributed verification of data flows.
2. For example, most of the state-level data breach notification laws in the US focus on whether there has been unauthorised acquisition of or access to protected data, ie whether the data has moved from one storage location to another or been transferred from one system or user to another. See, eg NY Gen. Bus. Law § 899-aa (defining 'breach of the security of the system' as 'unauthorized acquisition or acquisition without valid authorization of' protected information).
3. See, eg Del. Code Ann. tit. 6, § 12B-10 ('Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business').
4. Famously, the Federal Trade Commission Act — dating originally from 1914 and amended in 1938 — is silent as to information security, prohibiting rather 'unfair' or 'deceptive' acts in relation to commerce generally. See 15 U.S.C. § 45(a). The FTC's enforcement efforts in relation to information security have been upheld when challenged, however, with courts finding that an unfairness analysis, for example, is — by its very nature — flexible and dependent upon relevant circumstances. See *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 620 ('But the contour of an unfairness claim in the data-security context, like any other, is necessarily 'flexible' such that the FTC can apply Section 5 to the facts of particular cases arising out of unprecedented situations').
5. Compare 16 C.F.R. § 314.4 (the FTC's version of the Gramm-Leach-Bliley Act [GLBA] Safeguards Rule, specifically concerning the required elements of a comprehensive information security programme) and *In re Uber Technologies, Inc.*, FTC Docket No. C-4662, Revised Decision and Order (Oct. 25, 2018) (standard form of FTC consent decree in information security context adopting the five required elements of a GLBA comprehensive information security

program, found in § 314.4, albeit outside the ambit of GBLA).

6. Compare 45 C.F.R. § 312(e)(2)(ii) (identifying encryption of electronic Protected Health Information as 'addressable') with 23 N.Y.C.R.R. § 500.15 (requiring encryption of healthcare information, included within the regulation's definition of protected Nonpublic Personal Information, both in transit and at rest, unless 'infeasible').
7. Ponemon Institute (November 2018), 'Managing the Risk of Post-breach or "Resident" Attacks', p. 12. The study 'surveyed 627 IT and IT security practitioners in the United States to understand how well organizations are addressing cyber risks associated with attackers who may already be residing within the perimeter, including insiders that may act maliciously'. *Ibid.*, p. 1.
8. *Ibid.*, p. 12.
9. This trend toward lack of uniformity extends even to the pursuit of uniformity in regulatory approaches. For example, the National Association of Insurance Commissioners in the US has proposed a model law for regulating information security in the insurance space, MDL-668. See NAIC, 'Insurance Data Security Model Law', available at https://www.naic.org/store/free/MDL-668.pdf (accessed 29th May, 2019). States have begun to adopt this law, but with varying uniformity, such that each state that has adopted some form of the model law has created its own, unique version. For example, the South Carolina version of the model law requires entities covered under the law to give notice to the state insurance director within 72 hours of the entity detecting a defined cyber security event, see 'South Carolina Insurance Data Security Act', available at https://www.scstatehouse.gov/sess122_2017-2018/bills/4655.htm (accessed 29th May, 2019), while the Ohio version of the law requires notice to the Superintendent of Insurance within three business days, see 'Ohio Substitute Senate Bill No. 273, 132 Gen. Assembly', available at http://search-prod.lis.state.oh.us/solarapi/v1/general_assembly_132/bills/sb273/EN/06?format=pdf (accessed 29th May, 2019). The Michigan version of the model law allows ten business days for reporting. See 'Michigan Public Act 690, Pub. Acts of 2018', available at http://www.legislature.mi.gov/documents/2017-2018/publicact/pdf/2018-PA-0690.pdf (accessed 29th May, 2019).
10. Complexity even exists in the terminology used in these regulatory schemes to define their respective subject matters. Historically, 'information security' had been a common term used to define regulatory scope. See, eg 16 C.F.R. § 314.3 (requiring 'a comprehensive *information security* program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue' [emphasis added]). More recent efforts at regulation in this space have used the term 'cyber security', whether as useful shorthand for the longer term, 'information security', or as a linguistic symptom of how the prefix 'cyber' has come to mean anything connected with data or technology, albeit with a negative undertone. See, eg 23 N.Y.C.R.R. Part 500 (requiring a 'Cybersecurity Program'); see also, 'Where Is the Origin of "Cyber"?', available at https://blog.oxforddictionaries.com/2015/03/05/cyborgs-cyberspace-csi-cyber/ (accessed 29th May, 2019).
11. See, eg Fl. Stat. § 501.171 (Florida's data breach notification statute, defining 'covered entity' as 'a sole proprietorship, partnership, corporation, trust, estate, cooperative, association or other commercial entity that acquires, maintains, stores or uses personal information', regardless of geographic location).
12. See Ala. Code § 8-38-1 *et seq.* (Alabama Data Breach Notification Act of 2018, signed into law in March 2018, representing the last state to enact a data breach notification law).
13. Compare Ga. Code 10-1-911 and Ala. Code § 8-38-5.
14. For example, in 2017, Nationwide Mutual Insurance Company and its subsidiary, Allied Property & Casualty Insurance Company entered into a settlement with 33 states concerning an October 2012 data breach and agreeing to a fine of US$5.5m. See *In re Nationwide Mutual Insurance Company & Allied Property & Casualty Insurance Company*, Assurance of Voluntary Compliance, 3rd August, 2017, available at https://ag.ny.gov/sites/default/files/nationwide-aod.pdf (accessed 29th May, 2019).
15. See General Data Protection Regulation (GDPR) Art. 3.
16. See GDPR Recital 23.
17. See *Weltimmo v. NAIH* (C-230/14) at ¶¶ 31, 33 ('[T]he concept of "establishment" … extends to any real and effective activity — even a minimal one — exercised through stable arrangements. … The degree of stability of the arrangements and the effective exercise of activities must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned').
18. See, *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)* (C-131/12).
19. Similarly, there is no comprehensive listing of all entities that satisfy the other two prongs of the territorial scope test. For example, not all entities that offer goods or services to data subjects in the EU satisfy the offering-goods-or-services prong of Article 3. Only those that specifically 'envisage' doing so, eg those that have material sales to individuals in the Union or otherwise direct their efforts at obtaining such sales, are covered. Such a facts and circumstances test is, by definition, fluid, changing according business realities. For example, an app developer with immaterial EU sales one day can find itself squarely within the territorial scope of the GDPR the next day, if the developer's app goes globally viral.
20. See, eg 'GDPR Personal Data Definition: What You Need To Know', available at https://www.primitivelogic.com/insights/

gdpr-personal-data-definition-what-you-need-to-know/ (accessed 29th May, 2019) ('When we talk with companies about GDPR, many point to their current compliance with HIPAA or other data-compliance handling regulations. Or, they'll say something like, "We're not based in the EU, so it doesn't apply to us". However, it doesn't matter where your organization is located or incorporated. The bottom line is this: If you handle European Union residents' personal data, the General Data Protection Regulation [GDPR] requirements apply to you').

21. 201 C.M.R. 17.00 incorporates the main requirements of a GLBA information security programme, showing another jurisdiction applying GLBA-style rules outside the scope of GLBA.
22. See Nev. Rev. Stat. § 603A.030.
23. United States Census, available athttps://www.census.gov/quickfacts/de (accessed 29th May, 2019).
24. A full list of entities regulated by the New York State Department of Financial Services, and thereby potentially subject to Part 500, is available at https://www.dfs.ny.gov/about/whowesupervise.htm (accessed 29th May, 2019).
25. This interplay of privacy and cyber security regulation is an increasing trend. See, eg 23 N.Y.C.R.R. § 500.03 (including 'customer data privacy' as a required element to be addressed by a covered entity's 'Cybersecurity Policy').
26. Goldman, E. (July 2018), 'An Introduction to the California Consumer Privacy Act (CCPA)', p. 1, IAPP, available at https://iapp.org/media/pdf/resource_center/Intro_to_CCPA.pdf (accessed 29th May, 2019).
27. *Ibid*.
28. See 23 N.Y.C.R.R. Part 201 (Registration Requirements & Prohibited Practices for Credit Reporting Agencies).
29. 'Federal Online Data Security Regulation: Where Are We Going?', available at https://www.youtube.com/watch?v=GCxoQ445jLc&feature=youtu.be&t=6m40s (accessed 29th May, 2019) (videotaped comments of Commissioner Ohlhausen made before the Heritage Foundation).
30. See, eg Common Controls Hub, 'End Compliance Chaos', available at https://commoncontrolshub.com/ (accessed 29th May, 2019).
31. See, eg 23 N.Y.C.R.R. § 500.03 (incorporating the five functions of the NIST CSF Core, identify protect detect, respond and recover, into the Part 500 Cybersecurity Program requirement); see also, 'HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework', available at https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf (accessed 29th May, 2019).
32. See, eg https://www.nist.gov/document-3764 (accessed 29th May, 2019).
33. See GDPR Art. 42–43 (Certification and Certifying Bodies).
34. See Ohio Rev. Code Ann. § 1354.03.