A guide to US data protection

A mosaic of industry-focused federal data protection measures makes the United States' regime among the strictest in the world, writes Michelle Reed.

The mosaic of data protection laws in the United States is filled with various pieces – from federal to state laws and regulations – which blend together to create the whole that invokes privacy protection in the United States. Although there is no overarching federal data protection law like the European Union's General Data Protection Regulation ('GDPR'), the requirements surrounding data privacy and cybersecurity are well developed and industry specific. The United States has some of the strictest data breach notification standards in the world and these standards have been in place far longer than most other countries.

Underpinnings of US Data Privacy Law

Privacy protections in the United States have existed since the beginnings of the republic. The Constitution enshrines protections against unlawful intrusion into our homes and personal papers in the Fourth Amendment and other limitations on government intrusion into individual privacy in the First, Ninth, and Fourteenth Amendments.

'The Right to Privacy,' a 15 December 1890 article in the *Harvard Law Review* authored by attorney Samuel D. Warren and future US Supreme Court Justice, Louis Brandeis, became the first implicit declaration of a right to privacy in the United States. Privacy protections were first given to mail and then as new forms of communication developed, protections were extended to the telephone, the computer, and eventually email.

Over time, data protection in the United States became an intricate mosaic, with laws and regulations issued by both the federal government (at the national level) and state governments (at the state level). Federal law generally preempts state law on the same subject, though there are instances where the state law is not subject to federal preemption. Some laws apply to certain types of information (e.g., financial or health information) and others apply to use of information (e.g., telemarketing or commercial emails). At the national level, the Federal Trade Commission ('FTC'), an independent agency authorised to enforce against 'unfair and deceptive trade practices' has been the leader in developing and enforcing privacy protections. At the state level, state attorneys general lead the way with enforcing privacy and cybersecurity standards.

> The United States has some of the strictest data breach notification standards in the world and these standards have been in place far longer than most other countries.

In addition, there are many private industry groups that issue self-regulatory guidelines and frameworks, which have often been used as an enforcement framework for state and federal regulators. The National Institute of Standards and Technology ('NIST') issued its first 'Framework for Improving Critical Infrastructure Cybersecurity' in 2014. The framework continues to be updated and tailored to fit specific industries, and version 1.1 of the NIST Cybersecurity Framework was released in 2018. The NIST Cybersecurity Framework is often used as a benchmark for reasonable cybersecurity controls in both enforcement actions and litigation matters.

The FTC

The Federal Trade Commission Act ('FTCA')[1] is a broad consumer protection law that prohibits unfair or deceptive practices. The FTC has used this act to bring enforcement actions against companies failing to comply with posted privacy policies, unauthorised disclosure of personal data, and failure to enforce reasonable cybersecurity policies. The FTC's ability to enforce reasonable cybersecurity protections as an unfair trade practice was recently limited by the US Court of Appeals for the Eleventh

Circuit, which held that the lack of defined regulations in a cease and desist order did not provide companies with sufficient notice for compliance.[2] Despite this limitation, the FTC continues to be the preeminent regulator of privacy and data protection in the United States.

Industry regulations

Data protection regulation in the United States varies by industry. Industries that have a higher risk profile due to extensive use of personal data or unique risk of critical industries are more likely to be targeted by regulations.

Healthcare

As one of the longest standing areas of regulation, health privacy and cybersecurity is governed primarily by the Health Insurance Portability and Accountability Act ('HIPAA').[3] Health care providers, data processors, pharmacies, and other business associates are all subject to HIPAA, which defines specific standards for privacy ('the HIPAA Privacy Rule') and security ('the HIPAA Security Rule').[4] The HIPAA Breach Notification Rule[5] requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

Such notification must be made without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity or business associate. California's Confidentiality of Medical Information Act ('CMIA') provides stronger privacy protections for medical information than HIPAA.[6]

Financial services

Banks, securities firms, insurance companies, and other financial services organisations serve a key role in the economy and accordingly the privacy and cybersecurity protections mandated under both federal and state law are extensive. The Financial Services Modernization Act, more commonly known as the Gramm-Leach-Bliley Act ('GLB')[7] is the principal framework for

collection, use, and disclosure of financial information.

GLB prohibits disclosure of non-public personal information, which is more broadly defined than personally identifiable information and includes (1) any information an individual provides to obtain a financial product or service (e.g., name, address, income, social security number, or other information on an application); (2) any information about an individual from a transaction involving a financial product or service (e.g., the fact that an individual is a consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or (3) any information about an individual in connection with providing a financial product or service (e.g., information from court records or from a consumer report).

Companies subject to GLB are also required to provide notice of their privacy practices and an opportunity for data subjects to opt out of having their information shared with third parties.

Industries that have a higher risk profile due to extensive use of personal data or unique risk of critical industries are more likely to be targeted by regulations.

Various other federal agencies have also promulgated data protection rules such as the Safeguards Rule, Disposal Rule, and the Red Flags Rule for protecting and ensuring safe disposal of financial data.

In an attempt to force more rigorous security controls, the New York State Department of Financial Services ('NYDFS') passed its own cybersecurity regulations to apply to financial services companies that operate in New York, effective March 2017.[8] The NYDFS rules impose some of the most stringent security requirements of any state law or regulation, including a 72-hour data breach notification requirement, and have caused many financial services companies to take a deeper look at compliance.

Credit reporting agencies

In the United States, credit reporting agencies collect extensive information about the creditworthiness of consumers. These credit scores and reports can have a significant impact on access to credit and housing. In response to concerns about proper protections governing such a powerful tool, Congress passed the Fair Credit Reporting Act ('FCRA')[9], later amended by the Fair and Accurate Credit Transactions Act. FCRA regulates consumer reporting agencies, companies who use consumer reports (e.g., a lender), and companies that provide consumer-reporting information (e.g., a credit card company).

Following the data breach of 148 million consumers' information at Equifax – one of the largest consumer reporting agencies – there has been significant discussion of further regulation of consumer reporting agencies, though none has been enacted to date.

Marketing and advertising

The FTC has been the primary regulator for marketing and advertising, encouraging companies to implement four fair information practices: (1) giving consumers notice of a website's information practices; (2) offering consumers choice as to how their personally identifying information is used; (3) providing consumers with access to the information collected about them; and (4) ensuring the security of the information collected.

The FTC implies these principles from its unfair and deceptive trade practices jurisdiction through the FTCA. There have also been significant discussions in Congress about imposing additional regulations.

Even more stringent requirements are imposed by the Children's Online Privacy Protection Act ('COPPA'),[10] which is enforced by the FTC. COPPA requires websites to obtain verifiable parental consent before collecting, using, or disclosing personal information from children, including their names, home addresses, email addresses, or hobbies. The industry has also introduced self-regulatory principles for behavioural

advertising. As a general rule, 'opt out' consent is generally considered acceptable in the United States, with some exceptions for special types of data and classes of individuals.

States have also begun to regulate large data brokers. In May 2018, Vermont passed legislation to regulate data brokers, effective 1 January 2019. Data brokers will be required to register with the Vermont attorney general and pay a $100 registration fee; provide annual disclosures to the Vermont attorney general concerning data privacy practices and data breaches; and develop, implement, and maintain a comprehensive written information security programme that contains administrative, technical, and physical safeguards.

Energy

Security has been the primary focus of the energy industry, with extensive regulation for utilities. Electric grid regulations apply to utility companies under the Critical Infrastructure Protection ('CIP') Standards, issued by the North American Electric Reliability Corporation ('NERC') and approved by the Federal Energy Regulatory Commission. Oil and gas companies have not been subject to the same degree of scrutiny, even though the implementing recommendations of the 9/11 Commission Act of 2007[11] authorises the Department of Homeland Security's Transportation Safety Administration ('TSA') to issue pipeline security regulations if the TSA determines that doing so is necessary.

Privacy has also been an increased focus as many energy companies develop smart grid technologies.

Privacy has also been an increased focus as many energy companies develop smart grid technologies. The Smart Grid Data Privacy Voluntary Code of Conduct ('VCC') Initiative began in 2012, undertaken in partnership with the Federal Smart Grid Task Force (a multi-stakeholder effort involving utilities, regulatory bodies, consumer and privacy advocates, technology providers, and associations). The initiative developed the DataGuard Energy Data Privacy Program that provides utilities and third parties with a framework for handling and protecting customers' data and a way to communicate that commitment to customers.

Retail

The retail industry has been the source of significant privacy and cybersecurity threats – from the Target breach, which cost the company over $250 million, to the previously undisclosed Uber data breach of millions of customers' data, which caused a public relations crisis.

Regulation of credit card data in the United States is governed by the Payment Card Industry Data Security Standard ('PCI DSS'). This set of security standards is designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment. The enforcement mechanism is contractual – retailers have contracts with the major card brands that impose significant penalties for noncompliance.

Retailers also face close scrutiny from the FTC, particularly with the advent of the Internet of Things, which has further implications for data privacy. Other federal regulations, such as the Video Privacy Protection Act ('VPPA'),[12] provide further limitations on the wrongful disclosure of video tape rental or sale records [or similar audio visual materials, to cover items such as video games and the future DVD format] and have resulted in significant private litigation.

Government contracts

Government contractors face significant privacy and cybersecurity requirements under the Federal Acquisition Regulation ('FAR') and Defense Federal Acquisition Regulation Supplement ('DFARS') for classified information, controlled unclassified information, and covered defence information. Detailed NIST 800-171 standards are contractually required to be implemented into the contractors' security programmes, depending on the regulations to which the contractor is subject. The Department of Defense requires that contractors rapidly report any breaches within 72 hours.

The Department of Defense and other government agencies have also announced that they will continue to scrutinise contractors' supply chain security plans and programmes from proposal submission to contract closeout. The 2019 National Defense Authorization Act as approved by Congress and DHS initiatives highlight the government's increased focus on supply chain and cybersecurity requirements.

Data breach notification requirements

All 50 states and three territories have imposed laws that require notification of data breaches involving personally identifiable information. The standards are similar, but also inconsistent. In general, they require notification in a reasonable time period (which varies by state) of any breach of data that could lead to identity theft. Some generally define personally identifiable information and others provide other, specific combinations of data that require notice. Many, but not all, require notification of the state attorney general and some require notification of specific law enforcement agencies. Although legislation to enact a federal standard that would preempt state notification laws has been proposed in Congress, it has never passed, despite the transactional costs to companies of complying with 50 different standards.

Other state and federal regulations

There are a host of non-industry-specific regulations governing privacy. The Controlling the Assault of No-Solicited Pornography and Marketing Act ('CAN-SPAM Act')[13] and the Telephone Consumer Protection Act[14] were passed by Congress to curb unsolicited email and telephone calls, providing strict limitations on commercial emails and telephone calls to consumers. The Electronic Communications Privacy Act[15] and the Consumer Fraud and Abuse Act[16] make it illegal to intercept electronic communications and tamper with computers.

The Securities & Exchange Commission ('SEC') also issued rules regarding privacy and cybersecurity for public companies, broker dealers, and investment funds regulated by the industry. The SEC adopted Commission-level guidance on cybersecurity disclosures in 2018 and brought its first high-profile enforcement action and settlement for non-disclosure against Altaba, formerly known as Yahoo, for $35 million.

At the state level, certain states have

imposed more stringent data protection standards. For example, the Massachusetts 'Standards for The Protection of Personal Information of Residents of the Commonwealth'[17] includes strict requirements for data security: encryption of personal data; retention and storage of both digital and physical records; network security controls (e.g., firewalls); risk-management policies and practices; employee training; adequate documentation of data breaches; adequate documentation of any policy changes; and ensuring that any associated third-party providers who have access to the data maintain the same standards.

Government law enforcement and anti-terrorism efforts

The law continues to evolve on the government's access to private records. The Patriot Act is a United States statute that amended numerous existing laws to grant federal law enforcement and intelligence officers increased powers to obtain and share records for counter-terrorism purposes. Specifically, the Patriot Act allowed the Federal Bureau of Investigation ('FBI'), including when it is acting on behalf of the NSA (National Security Agency), to petition a Foreign Intelligence Surveillance Court ('FISA Court') for an order to obtain any business records. The Patriot Act was extended through 1 June 2015, but parts of the Patriot Act expired on 1 June 2015. The USA Freedom Act on 2 June 2015 then restored the expired parts and renewed them through 2019. While the government's ability to obtain records has been largely circumscribed by subsequent law, these powers remain a point of contention both in the United States and internationally.

The Supreme Court provided greater hope to privacy advocates in its decision in *Carpenter v. United States*,[18] the landmark decision concerning the privacy of historical cellphone location records. The court held, in a 5-4 decision authored by Chief Justice Roberts, that the government violates the Fourth Amendment to the United States Constitution by accessing historical records containing the physical locations of cellphones without a search warrant.

New developments

The closest analog to the GDPR in the United States is the recently passed California Consumer Protection Act. In July 2018, one of the largest states in the United States – California – passed a state law that requires businesses to tell customers about the personal data they collect, give consumers more control over how companies use and share their personal information, and provide consumers with a way to request data deletion. This law will not be effective until January 2020, and many anticipate that it will be amended before it goes into effect. The CCPA creates the following rights and enforcement mechanisms:

- Right to know all data collected on them, including what categories of data and why it is being acquired, before it is collected, and any changes to its collection
- Right to refuse the sale of their information
- Right to request deletion of their data
- Mandated right to opt in before the sale of information of children under 16
- Right to know the categories of third parties with whom their data is shared, as well as those from whom their data was acquired
- Enforcement by the attorney general of the State of California
- Private right of action should breach occur, to ensure companies keep their information safe

As currently drafted, the statute applies to 'any business that earns $25 million in revenue per year, sells 50,000 consumer records per year, or derives 50 percent of its annual revenue from selling personal information.' This includes businesses that collect or sell personal information from consumers in California, regardless of where the company itself is located. Based on the most recent census bureau data, it is estimated that more than a half a million companies in the United States will be subject to the CCPA. California has long been a leader in data privacy protections and the passage of the CCPA is viewed by many as a presage of things to come in other states.

Other states have issued recent data protection guidance as well, with Colorado enacting Colorado House Bill 1128 in May 2018, which strengthens consumer protections by requiring formal information security policies as well as increased oversight of third parties.

Conclusion

Although the United States is often criticised for the lack of a single federal law governing privacy and cybersecurity, the mosaic of laws governing different industries and uses of data provide detailed and strong protections. While new laws such as the CCPA will likely drive the United States to similar protections as the GDPR, it will be a long time before any overarching data protection laws are implemented at the national level. ■

Michelle Reed is a partner in the Dallas office of Akin Gump Strauss Hauer & Feld LLP, and is a co-leader of the firm's cybersecurity, privacy, and data protection practice.

mreed@akingump.com

Links and notes

1 15 USC. §§ 41-58
2 *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. June 6, 2018)
3 42 USC. § 1301
4 45 C.F.R. §§ 160, 164
5 45 C.F.R. §§ 164.400-414
6 Cal. Civ. Code §§ 56-56.37
7 15 USC. §§ 6801-6827
8 23 N.Y.C.R.R. 500
9 15 USC. § 1681
10 15 USC. §§ 6801-6827
11 6 USC. § 1207(f)
12 18 US Code § 2710
13 15 USC. §§ 7701-7713, 18 USC. § 1037
14 47 USC. § 227
15 18 USC. § 2510
16 18 USC. § 1030
17 201 C.M.R. § 17.00
18 No. 16-402, 585 US ___ (2018)

This article is reprinted from the September 2018 issue of Trade Security Journal.

www.tradesecurityjournal.com