

# Data Protection & Privacy



2018

GETTING THE  
DEAL THROUGH

GETTING THE  
DEAL THROUGH

# Data Protection & Privacy 2018

Publisher  
Gideon Roberton  
[gideon.roberton@lbresearch.com](mailto:gideon.roberton@lbresearch.com)

Subscriptions  
Sophie Pallier  
[subscriptions@gettingthedeathrough.com](mailto:subscriptions@gettingthedeathrough.com)

Senior business development managers  
Alan Lee  
[alan.lee@gettingthedeathrough.com](mailto:alan.lee@gettingthedeathrough.com)

Adam Sargent  
[adam.sargent@gettingthedeathrough.com](mailto:adam.sargent@gettingthedeathrough.com)

Dan White  
[dan.white@gettingthedeathrough.com](mailto:dan.white@gettingthedeathrough.com)

**Law**  
**Business**  
**Research**



Published by  
Law Business Research Ltd  
87 Lancaster Road  
London, W11 1QQ, UK  
Tel: +44 20 3708 4199  
Fax: +44 20 7229 6910

© Law Business Research Ltd 2017  
No photocopying without a CLA licence.  
First published 2012  
Sixth edition  
ISSN 2051-1280

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between June and August 2017. Be advised that this is a developing area.

Printed and distributed by  
Encompass Print Solutions  
Tel: 0844 2480 112

## CONTENTS

<b>Introduction</b>	<b>5</b>	<b>Luxembourg</b>	<b>106</b>
Wim Nauwelaerts Hunton & Williams		Marielle Stevenot and Audrey Rustichelli MNKS	
<b>EU overview</b>	<b>9</b>	<b>Mexico</b>	<b>113</b>
Wim Nauwelaerts and Claire François Hunton & Williams		Gustavo A Alcocer and Abraham Díaz Arceo Olivares	
<b>Safe Harbor and the Privacy Shield</b>	<b>12</b>	<b>Poland</b>	<b>119</b>
Aaron P Simpson Hunton & Williams		Arwid Mednis and Gerard Karp Wierzbowski Eversheds Sutherland	
<b>Australia</b>	<b>14</b>	<b>Portugal</b>	<b>126</b>
Alex Hutchens, Jeremy Perier and Eliza Humble McCullough Robertson		Helena Tapp Barroso, João Alfredo Afonso and Tiago Félix da Costa Morais Leitão, Galvão Teles, Soares da Silva & Associados	
<b>Austria</b>	<b>20</b>	<b>Russia</b>	<b>133</b>
Rainer Knyrim Knyrim Trieb Attorneys at Law		Ksenia Andreeva, Anastasia Dergacheva, Vasilisa Strizh and Brian Zimbler Morgan, Lewis & Bockius LLP	
<b>Belgium</b>	<b>28</b>	<b>Serbia</b>	<b>140</b>
Wim Nauwelaerts and David Dumont Hunton & Williams		Bogdan Ivanišević and Milica Basta BDK Advokati	
<b>Brazil</b>	<b>36</b>	<b>Singapore</b>	<b>145</b>
Ricardo Barreto Ferreira and Paulo Brancher Azevedo Sette Advogados		Lim Chong Kin and Charmian Aw Drew & Napier LLC	
<b>Chile</b>	<b>42</b>	<b>South Africa</b>	<b>159</b>
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya García Magliona & Cía Abogados		Danie Strachan and André Visser Adams & Adams	
<b>China</b>	<b>47</b>	<b>Spain</b>	<b>168</b>
Vincent Zhang and John Bolin Jincheng Tongda & Neal		Alejandro Padín, Daniel Caccamo, Katiana Otero, Francisco Marín and Álvaro Blanco J&A Garrigues	
<b>France</b>	<b>55</b>	<b>Sweden</b>	<b>174</b>
Benjamin May and Clémentine Richard Aramis		Henrik Nilsson Wesslau Söderqvist Advokatbyrå	
<b>Germany</b>	<b>63</b>	<b>Switzerland</b>	<b>181</b>
Peter Huppertz Hoffmann Liebs Fritsch & Partner		Lukas Morscher and Leo Rusterholz Lenz & Staehelin	
<b>India</b>	<b>69</b>	<b>Turkey</b>	<b>189</b>
Stephen Mathias and Naqeeb Ahmed Kazia Kochhar & Co		Ozan Karaduman and Bentley James Yaffe Gün + Partners	
<b>Ireland</b>	<b>75</b>	<b>United Kingdom</b>	<b>195</b>
Anne-Marie Bohan Matheson		Aaron P Simpson Hunton & Williams	
<b>Italy</b>	<b>84</b>	<b>United States</b>	<b>202</b>
Rocco Panetta and Federico Sartore Panetta & Associati		Lisa J Sotto and Aaron P Simpson Hunton & Williams	
<b>Japan</b>	<b>93</b>		
Akemi Suzuki and Tomohiro Sekiguchi Nagashima Ohno & Tsunematsu			
<b>Lithuania</b>	<b>99</b>		
Laimonas Marcinkevičius Juridicon Law Firm			

# United States

**Lisa J Sotto and Aaron P Simpson**

Hunton & Williams

---

## Law and the regulatory authority

### 1 Legislative framework

**Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?**

The US legislative framework for the protection of PII resembles a patchwork quilt. Unlike other jurisdictions, the US does not have a dedicated data protection law, but instead regulates primarily by industry, on a sector-by-sector basis. There are numerous sources of privacy law in the US, including laws and regulations developed at both the federal and state levels. These laws and regulations may be enforced by federal and state authorities, and many provide individuals with a private right to bring lawsuits against organisations they believe are violating the law.

### 2 Data protection authority

**Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.**

There is no single regulatory authority dedicated to overseeing data protection law in the US. At the federal level, the regulatory authority responsible for oversight depends on the law or regulation in question. In the financial services context, for example, the Consumer Financial Protection Bureau and various financial services regulators (as well as state insurance regulators) have adopted standards pursuant to the Gramm-Leach-Bliley Act (GLB) that dictate how firms subject to their regulation may collect, use and disclose non-public personal information. Similarly, in the healthcare context, the Department of Health and Human Services is responsible for enforcement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) against covered entities.

Outside of the regulated industries context, the Federal Trade Commission (FTC) is the primary federal privacy regulator in the US. Section 5 of the FTC Act, which is a general consumer protection law that prohibits ‘unfair or deceptive acts or practices in or affecting commerce’, is the FTC’s primary enforcement tool in the privacy arena. The FTC has used its authority under section 5 to bring numerous privacy enforcement actions for a wide range of alleged violations by entities whose information practices have been deemed ‘deceptive’ or ‘unfair’. Although section 5 does not give the FTC fining authority, it does enable the FTC to bring enforcement actions against alleged violators, and these enforcement actions typically have resulted in consent decrees that prohibit the company from future misconduct and often require audits biennially for up to 20 years. Under section 5, the FTC is able to fine businesses that have violated a consent decree.

At the state level, attorneys general also have the ability to bring enforcement actions for unfair or deceptive trade practices, or to enforce violations of specific state privacy laws. Some state privacy laws allow affected individuals to bring lawsuits to enforce violations of the law.

---

### 3 Breaches of data protection

**Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?**

In general, violations of federal and state privacy laws lead to civil, not criminal, penalties. The main exceptions are the laws directed at surveillance activities and computer crimes. Violations of the federal Electronic Communications Privacy Act (ECPA) (which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act) or the Computer Fraud and Abuse Act (CFAA) can lead to criminal sanctions and civil liability. In addition, many states have enacted surveillance laws that include criminal sanctions, in addition to civil liability, for violations.

Outside of the surveillance context, the US Department of Justice is authorised to criminally prosecute serious HIPAA violations. In circumstances where an individual knowingly violates restrictions on obtaining and disclosing legally cognisable health information, the DOJ may pursue criminal sanctions.

---

## Scope

### 4 Exempt sectors and institutions

**Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?**

There is no single regulatory authority dedicated to overseeing data protection law in the US. At the federal level, different privacy requirements apply to different industry sectors and data processing activities. These laws often are narrowly tailored and address specific data uses. For those entities not subject to industry-specific regulatory authority, the FTC has broad enforcement authority at the federal level, and attorneys general at the state level, to bring enforcement action for unfair or deceptive trade practices in the privacy context.

---

### 5 Communications, marketing and surveillance laws

**Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.**

Interception of communications is regulated primarily at the federal level by the ECPA, which is composed of the Wiretap Act, the Stored Communications Act and the Pen Register Act. The federal CFAA also prohibits certain surveillance activities, but is focused primarily on restricting other computer-related activities pertaining to hacking and computer trespass. At the state level, most states have laws that regulate the interception of communications.

There are only a handful of laws that specifically target the practice of electronic marketing and the relevant laws are specific to the marketing channel in question.

Commercial email is regulated at the federal level by the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM). There are also state laws regulating commercial email, but these laws are generally pre-empted by CAN-SPAM.

Telemarketing is regulated at the federal level by the Telephone Consumer Protection Act of 1991 (TCPA) and the Telemarketing and Consumer Fraud and Abuse Prevention Act, as well as regulations implemented by the FTC and the Federal Communications Commission (FCC). There are also state laws regulating telemarketing activities.

Text message marketing is regulated primarily by the TCPA and regulations implemented by the FCC.

Fax marketing is regulated by the TCPA, as amended by the Junk Fax Prevention Act of 2005, and state laws.

## 6 Other laws

### **Identify any further laws or regulations that provide specific data protection rules for related areas.**

In addition to the laws set forth above, there are numerous other federal and state laws that address privacy issues, including state information security laws and laws that apply to:

- consumer report information: the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act of 2003 (FACTA);
- children's information: the Children's Online Privacy Protection Act (COPPA);
- driver's information: the Driver's Privacy Protection Act of 1994;
- video rental records: the Video Privacy Protection Act; and
- federal government activities: the Privacy Act of 1974.

The Cybersecurity Information Sharing Act (CISA) authorises entities to engage in certain cybersecurity monitoring, defence practices and information-sharing activities for purposes of protecting against cybersecurity threats. To help companies secure their information and systems, CISA provides businesses with certain liability protections in connection with monitoring information systems for cybersecurity purposes, implementing cybersecurity defensive measures, and sharing cyber intelligence with other private entities and federal government agencies.

## 7 PII formats

### **What forms of PII are covered by the law?**

The US does not have a dedicated data protection law. Thus, the definition of PII varies depending on the underlying law or regulation. In the state security breach notification law context, for example, the definition of PII generally includes an individual's name plus his or her social security number, driver's licence number, or financial account number. In other contexts, such as FTC enforcement actions, GLB or HIPAA, the definition of PII is much broader. Although certain laws apply only to electronic PII, many cover PII in any medium, including hard copy records.

## 8 Extraterritoriality

### **Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?**

As a general matter, the reach of US privacy laws is limited to organisations that are subject to the jurisdiction of US courts as constrained by constitutional due process considerations. Determinations regarding such jurisdiction are highly fact-specific and depend on the details of an organisation's contacts with the US.

## 9 Covered uses of PII

### **Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners?**

Generally, US privacy laws apply to all processing of PII. There are no formal designations of 'controllers' and 'processors' under US law as there are in the laws of other jurisdictions. There are, however, specific laws that set forth different obligations based on whether an organisation would be considered a data owner or a service provider. The most prominent example of this distinction is found in the US state breach notification laws. Pursuant to these laws, it is generally the case that the owner of the PII is responsible for notifying affected individuals

of a breach, whereas a service provider is responsible for informing the data owner that it has suffered a breach affecting the data owner's data. Once a data owner has been notified of a breach by a service provider, the data owner, not the service provider, then must notify affected individuals.

## Legitimate processing of PII

### **10 Legitimate processing – grounds**

#### **Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?**

US privacy laws generally do not limit the retention of PII to certain specified grounds. There are, however, laws that may indirectly affect an organisation's ability to retain PII. For example, organisations that are collecting personal information online from California residents must comply with the California Online Privacy Protection Act. Pursuant to this law, and general consumer expectations in the US, the organisation must provide a privacy notice detailing the PII the company collects and how it is used. If the organisation uses the PII in materially different ways than those set forth in the privacy notice without providing notice and obtaining consent for such uses from the relevant consumers, these uses would likely be considered a deceptive trade practice under federal and state unfair competition laws.

### **11 Legitimate processing – types of PII**

#### **Does the law impose more stringent rules for specific types of PII?**

Since the US does not have a dedicated data protection law, there is no singular concept of 'sensitive data' that is subject to heightened standards. There are, however, certain types of information that generally are subject to more stringent rules, such as:

#### **Sensitive data in the security breach notification context**

To the extent an organisation maintains individuals' names plus their social security numbers, driver's licence numbers or financial account numbers, notification generally is required under state and federal breach notification laws to the extent the information has been acquired or accessed by an unauthorised third party.

#### **Consumer report information**

The FCRA seeks to protect the confidentiality of information bearing on the creditworthiness and standing of consumers. The FCRA limits the permissible purposes for which reports that contain such information (known as consumer reports) may be disseminated, and consumer reporting agencies must verify that anyone requesting a consumer report has a permissible purpose for receiving the report.

#### **Background screening information**

Many sources of information used in background checks are considered public records in the US, including criminal, civil court, bankruptcy, tax lien, professional licensing, workers' compensation and driving records. The FCRA imposes restrictions on the inclusion of certain public records in background screening reports when performed by consumer reporting agencies. Employers also can investigate job applicants and employees using internet search engines, but they must comply with their legal obligations under various labour and employment laws to the extent such laws restrict the use of the information. For instance, consideration of factors such as age, race, religion, disability, or political or union affiliation in making employment decisions can be the basis for a claim of unlawful discrimination under federal or state law.

#### **Health information**

HIPAA specifies permissible uses and disclosures of protected health information (PHI), mandates that HIPAA-covered entities provide individuals with a privacy notice and other rights, regulates covered entities' use of service providers (known as business associates), and sets forth extensive information security safeguards relevant to electronic PHI.

### **Children's information**

COPPA imposes extensive obligations on organisations that collect personal information from children under 13 years of age online. COPPA's purpose is to provide parents and legal guardians greater control over the online collection, retention and disclosure of information about their children.

### **State social security number laws**

Numerous state laws impose obligations with respect to the processing of SSNs. These laws generally prohibit:

- intentionally communicating SSNs to the general public;
- using SSNs on ID cards required for individuals to receive goods or services;
- requiring that SSNs be used in internet transactions unless the transaction is secure or the SSN is encrypted or redacted;
- requiring an individual to use an SSN to access a website unless another authentication device is also used; and
- mailing materials with SSNs (subject to certain exceptions).

A number of state laws also impose restrictions targeting specific SSN uses.

---

### **Data handling responsibilities of owners of PII**

---

#### **12 Notification**

##### **Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?**

For organisations not otherwise subject to specific regulation, the primary law requiring them to provide a privacy notice to consumers is California's Online Privacy Protection Act. This law requires a notice when an organisation collects personal information from individuals in the online and mobile contexts. The law requires organisations to specify in the notice:

- the categories of PII collected through the website;
- the categories of third-party persons or entities with whom the operator may share the PII;
- the process an individual must follow to review and request changes to any of his or her PII collected online, to the extent such a process exists;
- how the operator responds to web browser 'do not track' signals or similar mechanisms that permit individuals to exercise choice regarding the collection of their PII online over time and across third-party websites or online services, if the operator engages in such collection;
- whether third parties collect PII about individuals' online activities over time and across different websites when an individual uses the operator's website or online service;
- the process by which consumers who visit the website or online service are notified of material changes to the privacy notice for that website; and
- the privacy notice's effective date.

Delaware also has enacted a law, the Delaware Online and Privacy Protection Act, that requires operators of commercial internet services to provide similar information to their users when collecting PII online. In addition to the California and Delaware laws, there are other federal laws that require a privacy notice to be provided in certain circumstances, such as:

#### **COPPA**

Pursuant to the FTC's Children's Online Privacy Protection Rule, implemented pursuant to COPPA, operators of websites or online services that are directed to children under 13 years old, or who knowingly collect information from children online, must provide a conspicuous privacy notice on their site. The notice must include statutorily prescribed information, such as the types of personal information collected, how the operator will use the personal information, how the operator may disclose the personal information to third parties, and details regarding a parent's ability to review the information collected about a child and opt out of further information collection and use. In most cases, an operator that collects information from children online also must send a direct notice to parents that contains the information

set forth above along with a statement that informs parents the operator intends to collect the personal information from their child. The operator also must obtain verifiable parental consent prior to collecting, using or disclosing personal information from children.

#### **FCRA and FACTA**

The FCRA, as amended by FACTA, imposes several requirements on consumer reporting agencies to provide consumers with notices, including in the context of written disclosures made to consumers by a consumer reporting agency, identity theft, employment screening, pre-screened offers of credit or insurance, information sharing with affiliates, and adverse actions taken on the basis of a consumer report.

#### **GLB**

Financial institutions must provide an initial privacy notice to customers by the time the customer relationship is established. If the financial institution shares non-public personal information with non-affiliated third parties outside of an enumerated exception, the entity must provide each relevant customer with an opportunity to opt out of the information sharing. Following this initial notice, financial institutions subject to GLB must provide customers with an annual notice. The annual notice is a copy of the full privacy notice and must be provided to customers each year for as long as the customer relationship persists. For 'consumers' (individuals that have obtained a financial product or service for personal, family or household purposes but do not have an ongoing, continuing relationship with the financial institution), a notice generally must be provided before the financial institution shares the individual's non-public personal information with third parties outside of an enumerated exception. A GLB privacy notice must explain what non-public personal information is collected, the types of entities with whom the information is shared, how the information is used, and how it is protected. The notice also must indicate the consumer's right to opt out of certain information sharing with non-affiliated parties. In 2009, the federal financial regulators responsible for enforcing privacy regulations implemented pursuant to GLB released model forms for financial institutions to use when developing their privacy notices. Financial institutions that use the model form in a manner consistent with the regulators' published instructions are deemed compliant with the regulation's notice requirements. In 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act transferred GLB privacy notice rule-making authority from the financial regulatory agencies to the CFPB. The CFPB then restated the GLB implementing regulations, including those pertaining to the model form, in Regulation P.

#### **HIPAA**

The Privacy Rule promulgated pursuant to HIPAA requires covered entities to provide individuals with a notice of privacy practices. The Rule imposes several content requirements, including:

- the covered entities' permissible uses and disclosures of PHI;
- the individual's rights with respect to the PHI and how those rights may be exercised;
- a list of the covered entity's statutorily prescribed duties with respect to the PHI; and
- contact information for the individual at the covered entity responsible for addressing complaints regarding the handling of PHI.

---

#### **13 Exemption from notification**

##### **When is notice not required?**

Outside of the specifically regulated contexts discussed above, a privacy notice in the US must only be provided in the context of collecting personal information from consumers online. There is no requirement of general application that imposes an obligation on unregulated organisations to provide a privacy notice regarding its offline activities with respect to personal information.

---

#### **14 Control of use**

##### **Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?**

In the regulated contexts discussed above, individuals are provided with limited choices regarding the use of their information. The

choices are dependent upon the underlying law. Under GLB, for example, customers and consumers have a legal right to opt out of having their non-public personal information shared by a financial institution with third parties (outside an enumerated exception). Similarly, under the FCRA, as amended by FACTA, individuals have a right to opt out of having certain consumer report information shared by a consumer reporting agency with an affiliate, in addition to another opt-out opportunity prior to any use of a broader set of consumer report information by an affiliate for marketing reasons. Federal telemarketing laws and the CAN-SPAM Act give individuals the right to opt out of receiving certain types of communications, as do similar state laws.

In addition, California's Shine the Light Law requires companies that collect personal information from residents of California generally to either provide such individuals with an opportunity to know which third parties the organisation shared California consumers' personal information with for such third parties' direct marketing purposes during the preceding calendar year or, alternatively, to give the individuals the right to opt out of such third-party sharing.

As the primary regulator of privacy issues in the US, the FTC periodically issues guidance on pressing issues. In the FTC's 2012 report entitled 'Protecting Consumer Privacy in an Era of Rapid Change', the FTC set forth guidance indicating that organisations should provide consumers with choices with regard to uses of personal information that are inconsistent with the context of the interaction through which the organisation obtained the personal information. In circumstances where the use of the information is consistent with the context of the transaction, the FTC indicated that offering such choices is not necessary.

## **15 Data accuracy**

**Does the law impose standards in relation to the quality, currency and accuracy of PII?**

There is no law of general application in the US that imposes standards related to the quality, currency and accuracy of PII. There are laws, however, in specific contexts that contain standards intended to ensure the integrity of personal information maintained by an organisation. The FCRA, for example, requires users of consumer reports to provide consumers with notices if the user will be taking an adverse action against the consumer based on information contained in a consumer report. These adverse action notices must provide the consumer with information about the consumer's right to obtain a copy of the consumer report used in making the adverse decision and to dispute the accuracy or completeness of the underlying consumer report. Similarly, pursuant to the HIPAA Security Rule, covered entities must ensure, among other things, the integrity of electronic protected health information (ePHI).

## **16 Amount and duration of data holding**

**Does the law restrict the amount of PII that may be held or the length of time it may be held?**

US privacy laws generally do not impose direct restrictions on an organisation's retention of personal information. There are, however, thousands of records retention laws at the federal and state level that impose specific obligations on how long an organisation may (or must) retain records, many of which cover records that contain personal information.

## **17 Finality principle**

**Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?**

US privacy laws have not specifically adopted the finality principle. As a practical matter, organisations typically describe their uses of personal information collected from consumers in their privacy notices. To the extent an organisation uses the personal information it collects subject to such a privacy notice for materially different purposes than those set forth in the notice, it is likely that such a practice would be considered a deceptive trade practice under federal and state consumer protection laws.

## **18 Use for new purposes**

**If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?**

In the US, organisations must use the personal information they collect in a manner that is consistent with the uses set forth in the privacy notice. To the extent an organisation would like to use previously collected personal information for a materially different purpose, the FTC and state attorneys general would expect the organisation to first obtain opt-in consent from the consumer for such use. Where the privacy notice is required by a statute (eg, a notice to parents pursuant to COPPA), failure to handle the PII as described pursuant to such notice also may constitute a violation of the statute.

## **Security**

### **19 Security obligations**

**What security obligations are imposed on PII owners and service providers that process PII on their behalf?**

Similar to privacy regulation, there is no comprehensive national information security law in the US. Accordingly, the security obligations that are imposed on data owners and entities that process PII on their behalf depend on the regulatory context. These security obligations include:

#### **GLB**

The Safeguards Rule implemented pursuant to GLB requires financial institutions to 'develop, implement, and maintain a comprehensive information security program' that contains administrative, technical and physical safeguards designed to protect the security, confidentiality and integrity of customer information. The requirements of the Safeguards Rule apply to all non-public personal information in a financial institution's possession, including information about the institution's customers as well as customers of other financial institutions. Although the Safeguards Rule is not prescriptive in nature, it does set forth five key elements of a comprehensive information security programme:

- designation of one or more employees to coordinate the programme;
- conducting risk assessments;
- implementation of safeguards to address risks identified in risk assessments;
- oversight of service providers; and
- evaluation and revision of the programme in light of material changes to the financial institution's business.

#### **HIPAA**

The Security Rule implemented pursuant to HIPAA, which applies to ePHI, sets forth specific steps that covered entities and their service providers must take to:

- ensure the confidentiality, integrity, and availability of ePHI;
- protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
- protect against any reasonably anticipated uses or disclosures of ePHI; and
- ensure compliance with the Security Rule by the covered entity's workforce.

Unlike other US information security laws, the Security Rule is highly prescriptive and sets forth detailed administrative, technical and physical safeguards.

#### **State information security laws**

Laws in several US states, including California, impose general information security standards on organisations that maintain personal information. California's law, for example, requires organisations that own or license personal information about California residents to implement and maintain reasonable security procedures and practices to protect the information from unauthorised access, destruction, use, modification or disclosure. In addition, organisations that disclose personal information to non-affiliated third parties must contractually require those entities to maintain reasonable security procedures.

### **Massachusetts Standards for the Protection of Personal Information**

In 2008, Massachusetts issued regulations requiring any person who holds personal information about Massachusetts residents to develop and implement a comprehensive, written information security programme to protect the data. The regulations apply in the context of both consumer and employee information, and require the protection of personal data in both paper and electronic formats. Unlike the California law, the Massachusetts law contains certain specific data security standards, including required technical safeguards, on all private entities with Massachusetts consumers or employees.

### **New York Department of Financial Services Cybersecurity Regulation**

In 2017, the New York State Department of Financial Services (NYDFS) issued a regulation that establishes a robust set of cybersecurity requirements for financial services providers regulated by the NYDFS. The cybersecurity regulation applies to entities that operate under a NYDFS licence, registration or charter pursuant to New York banking, insurance or financial services law. The cybersecurity regulation requires such covered entities to maintain a comprehensive cybersecurity programme and implement certain processes and technical controls related to risk assessments, user access privileges, software security, system auditing and monitoring, data encryption, data disposal and retention, and cybersecurity incident response. In addition, the regulation assigns cybersecurity oversight responsibilities to senior officials and boards of directors and requires entities to report cybersecurity events to the NYDFS.

### **Nevada encryption law**

Nevada law requires that organisations doing business in Nevada and that accept payment cards must comply with the Payment Card Industry Data Security Standard. It requires that other organisations doing business in Nevada use encryption when transferring ‘any personal information through an electronic, non-voice transmission other than a facsimile to a person outside of the secure system of the data collector’, and moving ‘any data storage device containing personal information beyond the logical or physical controls of the data collector or its data storage contractor’.

### **State social security number laws**

Numerous state laws impose obligations with respect to the processing of SSNs. These laws generally prohibit:

- intentionally communicating SSNs to the general public;
- using SSNs on ID cards required for individuals to receive goods or services;
- requiring that SSNs be used in internet transactions unless the transaction is secure or the SSN is encrypted or redacted;
- requiring an individual to use an SSN to access a website unless another authentication device is also used; and
- mailing materials with SSNs (subject to certain exceptions).

A number of state laws also impose restrictions targeting specific SSN uses.

---

### **20 Notification of data breach**

#### **Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?**

There are no breach notification laws of general application at the federal level. There are, however, numerous targeted breach notification laws at both the state and federal level, including:

#### **State breach laws**

At present, 47 states, the District of Columbia, the US Virgin Islands, Guam and Puerto Rico have enacted breach notification laws that require data owners to notify affected individuals in the event of unauthorised access to or acquisition of personal information, as that term is defined in each law. In addition to notification of individuals, the laws of 23 states also require notice to a state regulator in the event of a breach, typically the state attorney general. Although most state breach

laws require notification only if there is a reasonable likelihood that the breach will result in harm to affected individuals, a number of jurisdictions do not employ such a harm threshold and require notification of any incident that meets their definition of a breach.

### **Federal Interagency Guidance**

Several federal banking regulators issued the Interagency Guidance on Response Programs for Unauthorised Access to Customer Information and Customer Notice. Entities regulated by the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision are subject to the Interagency Guidance. The Interagency Guidance sets forth that subject financial institutions develop and implement a response programme to address incidents of unauthorised access to customer information processed in systems the institutions or their service providers use to access, collect, store, use, transmit, protect, or dispose of the information. In addition, the Interagency Guidance contains two key breach notification requirements. First, when a financial institution becomes aware of an incident involving unauthorised access to or use of sensitive customer information, the institution must promptly notify its primary federal regulator. Second, the institution must notify appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate attention. Third, the institution also must notify relevant customers of the incident if the institution’s investigation determines that misuse of sensitive customer information has occurred or is reasonably possible. In this context, ‘sensitive customer information’ means a customer’s name, address, or telephone number in conjunction with the customer’s SSN, driver’s licence number, account number, credit or debit card number, or a PIN or password that would permit access to the customer’s account. Any combination of these data elements that would allow an unauthorised individual to access the customer’s account also would constitute sensitive customer information.

### **HITECH Act**

The Health Information Technology for Economic and Clinical Health Act’s (HITECH Act) information security breach provisions apply in the healthcare context, governing both HIPAA-covered entities and non-HIPAA covered entities. The HITECH Act and the breach-related provisions of the HHS regulations implementing the Act require HIPAA-covered entities that experience an information security breach to notify affected individuals, and service providers of HIPAA-covered entities to notify the HIPAA-covered entity following the discovery of a breach. Unlike the state breach notification laws, the obligation to notify as a result of an information security breach under the HITECH Act falls on any HIPAA covered entity that ‘accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI’. Any HIPAA-covered entity that processes unsecured PHI must notify affected individuals in the event of a breach, whether the covered entity owns the data or not.

---

### **Internal controls**

---

#### **21 Data protection officer**

##### **Is the appointment of a data protection officer mandatory? What are the data protection officer’s legal responsibilities?**

No, the appointment of a data protection officer is not mandatory. Many organisations in the US appoint a Chief Privacy Officer, but his or her responsibilities are dictated by business need rather than legal requirements.

---

#### **22 Record keeping**

##### **Are owners of PII required to maintain any internal records or establish internal processes or documentation?**

There are no legal requirements of general application that obligate owners of PII to maintain internal records or establish internal processes or documentation. As discussed in question 19, there are several statutory frameworks in the US that require organisations to develop an information security programme, which typically must contain internal processes and documentation. These include requirements imposed by GLB, HIPAA and state information security laws.

**Registration and notification****23 Registration**

**Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?**

There are no registration requirements for data processing activities in the US.

**24 Formalities**

**What are the formalities for registration?**

There are no registration requirements for data processing activities in the US.

**25 Penalties**

**What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?**

There are no registration requirements for data processing activities in the US.

**26 Refusal of registration**

**On what grounds may the supervisory authority refuse to allow an entry on the register?**

There are no registration requirements for data processing activities in the US.

**27 Public access**

**Is the register publicly available? How can it be accessed?**

There are no registration requirements for data processing activities in the US.

**28 Effect of registration**

**Does an entry on the register have any specific legal effect?**

There are no registration requirements for data processing activities in the US.

**Transfer and disclosure of PII****29 Transfer of PII**

**How does the law regulate the transfer of PII to entities that provide outsourced processing services?**

As a general matter, organisations address privacy and information security concerns in their agreements with service providers that will provide outsourced processing services. There are no laws of general application in the US that impose requirements on data owners with respect to their service providers. There are, however, specific laws that address this issue, such as:

**HIPAA**

Through the Privacy and Security Rules, HIPAA imposes significant restrictions on the disclosure of PHI. The regulations require covered entities to enter into business associate agreements containing statutorily mandated language before PHI may be disclosed to a service provider.

**GLB**

In accordance with the Privacy Rule enacted pursuant to GLB, prior to disclosing consumer non-public personal information to a service provider, a financial institution must enter into a contract with the service provider prohibiting the service provider from disclosing or using the information other than to carry out the purposes for which the information was disclosed. Under the Safeguards Rule enacted pursuant to GLB, prior to allowing a service provider access to customer personal information, the financial institution must take reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards, and require the service provider by contract to implement and maintain such safeguards.

**State information security laws**

A number of states impose a general information security standard on businesses that maintain personal information. These states have laws requiring companies to implement reasonable information security measures. California law and Massachusetts law require organisations that disclose personal information to service providers to include contractual obligations that those entities maintain reasonable security procedures.

**30 Restrictions on disclosure**

**Describe any specific restrictions on the disclosure of PII to other recipients.**

A wide variety of laws contain disclosure restrictions targeted to specific forms of PII. For example, HIPAA and GLB impose limitations on certain disclosures, such as requirements for consent and for contracts with certain types of recipients.

**31 Cross-border transfer**

**Is the transfer of PII outside the jurisdiction restricted?**

US privacy laws do not impose restrictions on cross-border data transfers.

**32 Notification of cross-border transfer**

**Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?**

US privacy laws do not impose restrictions on cross-border data transfers.

**33 Further transfer**

**If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?**

US privacy laws do not impose restrictions on cross-border data transfers.

**Rights of individuals****34 Access**

**Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.**

There are no laws of general application in the US that provide individuals with a right to access the personal information about them that is held by an organisation. There are specific laws that address access rights, including:

**HIPAA**

Under the Privacy Rule enacted pursuant to HIPAA, an individual has a right to access PHI about the individual that is maintained by the covered entity unless the covered entity has a valid reason for denying the individual such access. Valid reasons can include the fact that the PHI is subject to restricted access under other laws, or that access to the PHI is reasonably likely to cause substantial harm to another person. A covered entity must provide the requested access to the PHI within 30 days of the request and must explain the justification for any denial of access.

**California's Shine the Light Law**

Under this law, organisations that collect personal information from California residents generally must either: (i) provide such individuals with an opportunity to know which third parties the organisation shared California consumers' personal information with for such third parties' direct marketing purposes during the prior calendar year; or (ii) allow such individuals the right to opt out of most third-party sharing. If an organisation implements option (i), it must provide California residents with a postal address, email address or toll-free telephone or fax number that California residents may contact to obtain the list of relevant third parties. Organisations are required to respond only to a single request per California resident per calendar year.

**COPPA**

This law allows parents or legal guardians to obtain access to the personal information that has been collected online from their children.

**35 Other rights****Do individuals have other substantive rights?**

There are no laws of general application in the US that provide individuals with other substantive rights. Some sector-specific laws provide such rights. For example, the HIPAA Privacy Rule does provide individuals with the right to amend their PHI. If an individual requests that a covered entity amend the individual's PHI, the covered entity must do so within 60 days of the request and must explain any reasons for denying the request. The FCRA provides individuals with the right to dispute and demand correction of information about them that is held by consumer reporting agencies.

**36 Compensation****Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?**

Individuals are entitled to monetary damages for wrongful acts under common law and pursuant to most statutes that provide for a private right of action. Consumers often bring class action lawsuits against organisations as a result of alleged privacy violations, such as statutory violations or other wrongful acts that affect them, such as information security breaches. In security breach cases, consumers often allege that the organisation was negligent in securing the consumers' personal information, and that such negligence led to the security breach. As a general matter, consumers would need to establish that they suffered actual damages as a direct result of the organisation's negligence in order to succeed on their claim.

In the regulatory context, the ability to obtain monetary damages or compensation depends entirely on the statute in question. Pursuant to the FCRA, for example, in the event an organisation is wilfully non-compliant with the law, the Act provides for the recovery by aggrieved individuals of actual damages sustained or damages of 'not less than \$100 and not more than \$1,000' per violation, plus punitive damages, attorneys' fees and court costs. Negligent non-compliance may result in liability for actual damages as well as costs and attorneys' fees. Other laws, such as section 5 of the FTC Act, provide no private right of action to individuals and instead can be enforced solely by the regulator.

**37 Enforcement****Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?**

To the extent an individual obtains monetary relief as a result of illegal activity by an organisation, that relief will be obtained primarily through the judicial system. Typically, the civil penalties imposed by regulators are not paid directly to aggrieved individuals. There are,

however, exceptions to this rule. For example, under the FCRA, organisations that settle claims with regulators can be asked to provide funds for consumer redress.

**Exemptions, derogations and restrictions****38 Further exemptions and restrictions****Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.**

There is no law of general application regarding privacy and information security in the US, and thus there are no derogations, exclusions or limitations of general application as there are in other jurisdictions. CISA provides companies with liability protection for cybersecurity monitoring and defence practices. For example, CISA preempts state law and grants liability protection to companies against any cause of action in any court for the monitoring of an information system and information to the extent the monitoring is conducted for cybersecurity purposes delineated under CISA.

**Supervision****39 Judicial review****Can PII owners appeal against orders of the supervisory authority to the courts?**

The ability of an organisation to appeal orders of a supervisory authority is highly contextual. In the FTC context, an order is the result of an administrative proceeding before an FTC administrative law judge and the full FTC on review. An order issued by the FTC as a result of this process can be appealed directly to a federal court of appeals, where the FTC's order would be entitled to some deference on review.

**Specific data processing****40 Internet use****Describe any rules on the use of 'cookies' or equivalent technology.**

As of August 2016, this is a hot-button issue in the US, and regulation is evolving rapidly. There have been numerous legislative efforts aimed at providing formal regulation for the use of cookies, particularly in the behavioural advertising context. To date, none of those legislative efforts has succeeded. The FTC has issued a substantial amount of guidance in the area of online behavioural advertising, and industry has responded with a series of self-regulatory frameworks. Although not focused directly on cookies, there have been a number of civil actions brought by individuals and regulatory enforcement actions brought by the FTC for practices that depend on the use of cookies, but the allegations tend to focus on laws of more general application, such as surveillance laws and section 5 of the FTC Act.



**Lisa J Sotto**  
**Aaron P Simpson**

200 Park Avenue  
New York  
New York 10166  
United States

[lsotto@hunton.com](mailto:lsotto@hunton.com)  
[asimpson@hunton.com](mailto:asimpson@hunton.com)

Tel: +1 212 309 1000  
Fax: +1 212 309 1100  
[www.hunton.com](http://www.hunton.com)

**41 Electronic communications marketing**

Describe any rules on marketing by email, fax or telephone.

See question 5.

**42 Cloud services**

Describe any rules or regulator guidance on the use of cloud computing services.

There are no rules or regulator guidance specific to the use of cloud computing services.







## *Getting the Deal Through*

Acquisition Finance  
Advertising & Marketing  
Agribusiness  
Air Transport  
Anti-Corruption Regulation  
Anti-Money Laundering  
Arbitration  
Asset Recovery  
Automotive  
Aviation Finance & Leasing  
Banking Regulation  
Cartel Regulation  
Class Actions  
Commercial Contracts  
Construction  
Copyright  
Corporate Governance  
Corporate Immigration  
Cybersecurity  
Data Protection & Privacy  
Debt Capital Markets  
Dispute Resolution  
Distribution & Agency  
Domains & Domain Names  
Dominance  
e-Commerce  
Electricity Regulation  
Energy Disputes  
Enforcement of Foreign Judgments  
Environment & Climate Regulation

Equity Derivatives  
Executive Compensation & Employee Benefits  
Financial Services Litigation  
Fintech  
Foreign Investment Review  
Franchise  
Fund Management  
Gas Regulation  
Government Investigations  
Healthcare Enforcement & Litigation  
High-Yield Debt  
Initial Public Offerings  
Insurance & Reinsurance  
Insurance Litigation  
Intellectual Property & Antitrust  
Investment Treaty Arbitration  
Islamic Finance & Markets  
Labour & Employment  
Legal Privilege & Professional Secrecy  
Licensing  
Life Sciences  
Loans & Secured Financing  
Mediation  
Merger Control  
Mergers & Acquisitions  
Mining  
Oil Regulation  
Outsourcing  
Patents  
Pensions & Retirement Plans

Pharmaceutical Antitrust  
Ports & Terminals  
Private Antitrust Litigation  
Private Banking & Wealth Management  
Private Client  
Private Equity  
Product Liability  
Product Recall  
Project Finance  
Public-Private Partnerships  
Public Procurement  
Real Estate  
Restructuring & Insolvency  
Right of Publicity  
Securities Finance  
Securities Litigation  
Shareholder Activism & Engagement  
Ship Finance  
Shipbuilding  
Shipping  
State Aid  
Structured Finance & Securitisation  
Tax Controversy  
Tax on Inbound Investment  
Telecoms & Media  
Trade & Customs  
Trademarks  
Transfer Pricing  
Vertical Agreements

*Also available digitally*



# Online

[www.gettingthedealthrough.com](http://www.gettingthedealthrough.com)



Data Protection & Privacy  
ISSN 2051-1280



THE QUEEN'S AWARDS  
FOR ENTERPRISE:  
2012



Official Partner of the Latin American  
Corporate Counsel Association



Strategic Research Sponsor of the  
ABA Section of International Law