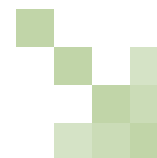


United States

leuan Jolly, Loeb & Loeb LLP



www.practicallaw.com/2-385-9889

REGULATION

1. What national law(s) apply to the collection and use of personal data? If applicable, has Directive 95/46/EC on data protection (Data Protection Directive) been implemented?

There is no single, comprehensive federal (national) law regulating the collection and use of personal data. Instead, the US has a patchwork system of federal and state laws and regulations that overlap, dovetail and can sometimes contradict one another. In addition, there are many guidelines, developed by government agencies as well as industry groups, that do not have the force of law but are part of self-regulatory efforts and are considered best practices. The proliferation of security breaches in recent years has led to an expansion of this patchwork system, which is now becoming one of the fastest growing areas of legal regulation. The increase in inter-state and cross-border data flow, together with the increased enactment of data protection related statutes, heightens the risk of privacy violations and creates a significant challenge for data controllers trying to navigate the disharmonious patchwork of federal and state laws regulating the collection and processing of personal data.

Federal privacy laws

There are many national laws that regulate the collection and use of personal data. Some apply to particular categories of information, such as financial or health information or electronic communications. Others apply to activities that use personal information, such as telemarketing and commercial email. In addition, there are broad consumer protection laws that are not privacy laws per se, but have been used to prohibit unfair or deceptive practices involving the disclosure of, and security procedures for protecting, personal information.

Some of the most prominent federal privacy laws include the:

- Federal Trade Commission Act (15 U.S.C. §§41-58) (FTC Act). This is a federal consumer protection law that prohibits unfair or deceptive practices and has been applied to offline and online privacy and data security policies. The Federal Trade Commission (FTC) is very active in the privacy area and has brought many enforcement actions against companies for failing to comply with posted privacy policies and for the unauthorized disclosure of personal data. The FTC is the primary enforcer of the Children's Online Privacy Protection Act (15 U.S.C. §§6501-6506), which applies to the online collection of information from children, and recently issued Self-Regulatory Principles for Behavioural Advertising.
- Financial Services Modernization Act (15 U.S.C. §§6801-6827) (Gramm-Leach-Bliley Act or GLB) regulates the collection, use and disclosure of financial information. It applies very broadly to financial institutions such as banks, securities firms and insurance companies, and to other businesses that provide financial services and products. GLB limits the disclosure of non-public personal information, and in some cases requires financial institutions to provide notice of their privacy practices and an opportunity for data subjects to opt-out of having their information shared. In addition, there are several Privacy Rules promulgated by national banking agencies and the Safeguards Rule, Disposal Rule, and Red Flags Rule issued by the FTC that relate to the protection and disposal of financial data.
- Health Insurance Portability and Accountability Act (42 U.S.C. §1301 et seq.) (HIPAA) governs medical information. It applies broadly to health care providers, data processors, pharmacies and other entities that come into contact with medical information. The Standards for Privacy of Individually Identifiable Health Information (HIPAA Privacy Rule) (45 C.F.R. Parts 160 and 164) apply to the collection and use of protected health information (PHI). The Security Standards for the Protection of Electronic Protected Health Information (HIPAA Security Rule) (45 C.F.R. 160 and 164) provide standards for protecting medical data. The Standards for Electronic Transactions (HIPAA Transactions Rule) (45 C.F.R. 160 and 162) apply to the electronic transmission of medical data. The recently enacted American Recovery and Reinvestment Act of 2009 directs the Department of Health and Human Services to develop rules requiring HIPAA-covered entities, such as hospitals, doctors' offices, and health insurance plans, to notify individuals if there is a security breach and would require business associates of HIPAA-covered entities to notify such covered entities in the event of a security breach. The FTC is developing a similar rule for companies that are not regulated by HIPAA but are developing and distributing online and offline applications that interact with personal health records.
- Fair Credit Reporting Act (15 U.S.C. §1681) (and the Fair and Accurate Credit Transactions Act (Pub. L. No. 108-159) which amended the Fair Credit Reporting Act) applies to consumer reporting agencies, those who use consumer reports (such as a lender) and those who provide consumer reporting information (such as a credit card company). Consumer reports are any communication issued by a consumer reporting agency, relating to a consumer's credit worthiness, credit history, credit capacity, character, and general reputation, used to evaluate a consumer's eligibility for credit or insurance.

- Controlling the Assault of Non-Solicited Pornography and Marketing Act (also known as the CAN-SPAM Act) (15 U.S.C. §§7701-7713 and 18 U.S.C. §1037) and the Telephone Consumer Protection Act (47 U.S.C. §227 et seq.) regulate the collection and use of email addresses and telephone numbers, respectively.
- Electronic Communications Privacy Act (18 U.S.C. §2510) and the Computer Fraud and Abuse Act (18 U.S.C. §1030) govern the interception of electronic communications and computer tampering, respectively. A class action complaint filed in late 2008 alleged Internet Service Providers (ISPs) and a targeted advertising company violated these statutes by intercepting data sent between individuals' computers and ISP servers (known as "deep packet inspection"). This is the same practice engaged by Phorm in the UK and several UK telecommunications companies that resulted in an investigation by the European Commission (Commission).

There are also many federal security and law enforcement laws that regulate the use of personal information, but these laws are outside the scope of this chapter.

In addition to the above laws, there are also many guidelines issued by industry groups that do not have the force of law, but are generally considered best practices in those industries (such as the payment card, mobile marketing, and online advertising industries). For example, the Mobile Marketing Association Guidelines suggest that mobile marketers (that is, companies advertising on mobile or wireless devices) ask for and obtain an explicit opt-in for all mobile messaging programmes and should implement a simple opt-out process, and they should implement reasonable technical, administrative and physical procedures to protect user information from unauthorised use, disclosure or access.

State privacy laws

There are hundreds of laws at the state level with inconsistent scope and obligations that address unauthorised access to personal information and security breaches and regulate the collection and use of personal data, some of which are pre-empted by federal privacy laws on the same topic, which compounds the challenge for data controllers trying to find a road-map for privacy compliance in the US.

Most states have enacted some form of privacy legislation, however California paves the way in the privacy arena, having enacted multiple privacy laws, some of which have far-reaching effects at a national level. Unlike many federal privacy laws in the US, California's privacy laws resemble the European approach to privacy protection. California laws typically require an opt-in standard, provide consumers with the ability to learn how their personal information is used, and allow consumers (as individuals or as part of a class) to file suit to enforce these laws. For example, the "Shine the Light" law requires companies to disclose details of the third parties with whom they have shared their personal information, and the data security law requires businesses to implement and maintain "reasonable security procedures" to protect personal information from unauthorised access, destruction, use, modification, or disclosure. California is one of only a handful of states to create an Office of Privacy Protection (www.privacy.ca.gov).

California was also the first state to enact a security breach notification law (California Civil Code §1798.82) which requires any person or business that owns or licenses computerised data that includes personal information to disclose any breach of the security of the system to all California residents whose unencrypted personal information was acquired by an unauthorised person. This law dramatically changed the privacy landscape in the US because consumers were notified for the first time of data breaches, and subsequently 43 other states followed California's lead and enacted similar laws.

Most of the early state security breach notification laws mirrored California's law, but more recently states have enacted more stringent security breach notification laws. For example, Massachusetts recently enacted a law (MGL 93H) that requires businesses, whether located in or outside of Massachusetts, that maintain personal information about Massachusetts residents to use encryption and firewalls, develop, implement and maintain a comprehensive written information security program, and verify that any third-party service provider that has access to personal information can protect such information.

As of January, 2009, 44 states, as well as the District of Columbia, Puerto Rico and the Virgin Islands all have enacted laws requiring notification of security breaches involving personal information.

This chapter will focus on the FTC Act and several rules and principles enforced by the FTC, the GLB Act, regulating financial information, HIPAA, regulating medical information, and two of the most prominent state laws on which many subsequent state laws have been mirrored: California's Security Breach Notification Law and California's Online Privacy Protection Act.

2. To whom do the rules apply (EU: data controller)?

The FTC Act applies to most companies and individuals doing business in the US, other than certain transportation, telecommunications and financial companies (because these industries are primarily regulated by other national agencies). Compliance with the FTC's Behavioural Advertising Principles is voluntary, although many companies consider them best practices. They apply to website operators that engage in behavioural advertising (also called contextual advertising and targeted advertising).

GLB applies to "financial institutions", broadly defined to include any institution engaging in "financial activities", such as banks, securities firms, and insurance companies. According to the FTC, an institution must be "significantly engaged" in financial activities to be considered a financial institution. Whether a financial institution is significantly engaged in financial activities is a flexible standard that takes into account all the facts and circumstances. GLB also applies to third parties that are not financial institutions, but that receive non-public personal information from non-affiliated financial institutions.

HIPAA applies to "covered entities" and "business associates". Covered entities include health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically. A business associate is a person or entity that performs certain functions or activities that

involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity. Such activities include claims processing or administration, data analysis and processing, quality assurance, billing, benefit management, practice management and re-pricing.

The California Security Breach Notification Law applies to any person or business that conducts business in California and that owns or licenses computerised data that includes personal information.

The California Online Privacy Protection Act applies to commercial website or online service operators that collect personally identifiable information through the internet about individual consumers residing in California, who use or visit its commercial website or online service.

3. What data is regulated (EU: personal data)?

The FTC Act does not regulate categories of data. Instead, it prohibits unfair or deceptive acts or practices that affect consumers' personal information. The FTC's Behavioural Advertising Principles apply to "the tracking of a consumer's activities online over time - including the searches the consumer has conducted, the web pages visited, and the content viewed - in order to deliver advertising targeted to the individual consumer's interests".

GLB applies to non-public personal information collected by a financial institution that is provided by, results from, or is otherwise obtained in connection with consumers and customers who obtain financial products or services primarily for personal, family or household purposes from a financial institution. A "consumer" is someone who has obtained a financial product or service, but does not have an ongoing relationship with the financial institution (for example, someone who cashed a check with a check-cashing company or made a wire transfer or applied for a loan). A "customer" is a sub-set of consumers, and refers to someone with an ongoing relationship with the institution. The non-public personal information that is the subject of GLB applies to information which is not publicly available and which is capable of personally identifying a consumer or customer.

HIPAA regulates PHI which is individually identifiable health and medical information that is maintained or transmitted by a covered entity or its business associate.

The California Security Breach Notification Law regulates "personal information" which means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number.
- Driver's licence number or California Identification Card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would allow access to an individual's financial account.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

The California Online Privacy Protection Act defines "personally identifiable information" as individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following:

- A first and last name.
- A home or other physical address, including street name and name of a city or town.
- An email address.
- A telephone number.
- A social security number.
- Any other identifier that permits the physical or online contacting of a specific individual.
- Information concerning a user that the website or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described above.

4. What acts are regulated (EU: processing)?

The FTC Act prohibits unfair or deceptive acts or practices. The FTC has used its authority to charge companies that fail to protect consumer personal data or that have changed their privacy policies without adequate notice, or that fail to comply with a posted privacy policy.

GLB regulates the collection, use, sharing and disclosure of non-public financial information. The requirements for written notice of privacy procedures and obtaining consent (and opportunities to opt-out of certain disclosures) vary depending on whether the data subject is a "customer" or a "consumer", and with whom the financial institution shares such information. One of the most onerous obligations is implementing a security programme to protect the non-public personal information from unauthorised disclosures.

HIPAA regulates the use and disclosure of PHI and the collection, use, maintenance, or transmission of electronic PHI, and requires notice of privacy practices.

The California Security Breach Notification Law requires any person or business that conducts business in California and owns or licenses computerised data that includes personal information to disclose any security breach of such information following discovery or notification of the breach to any Californian resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person. In addition, any person or business that maintains computerised data that includes personal information that the person or business does not own must notify the owner or licensee of the information of any breach of the security of the data immediately following dis-

covery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorised person.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes the information handling procedures of such website.

5. What is the jurisdictional scope of the rules?

The FTC Act and rules and guidelines promulgated under the FTC's authority apply to companies and individuals doing business in the US.

GLB applies to financial institutions (which is defined very broadly, see *Question 2*) and to affiliated and non-affiliated third parties that receive non-public personal information from financial institutions, and to persons who obtain or attempt to obtain, or cause or attempt to cause disclosure of, that non-public personal information from financial institutions through false or fraudulent means.

The jurisdictional scope of HIPAA is limited to covered entities (see *Question 2*) over which the US government has enforcement authority. However, certain business associates of covered entities may have contractual obligations to safeguard PHI, including those operating outside of the US jurisdiction.

The California Security Breach Notification Law applies to any person or business that conducts business in California, and that owns or licenses computerised data that includes personal information.

California Online Privacy Protection Act applies to an operator of a commercial website or online service that collects personally identifiable information through the internet about individual consumers residing in California who use or visit its commercial website or online service.

6. What are the main exemptions (if any)?

The privacy rules and guidelines issued by the FTC provide exemptions from privacy requirements for law enforcement purposes.

Under GLB, a financial institution can disclose a consumer's non-public personal information with an affiliated entity if it provides notice of this practice. The financial institution does not need to obtain consent for this disclosure. An affiliated entity is "any company that controls, or is controlled by, or is under common control with another company" and includes financial and non-financial institutions.

A financial institution can disclose a consumer's non-public personal information with a non-affiliated entity without providing the consumer the right to opt-out if:

- The disclosure is to a third party that uses the information to perform services for the financial institution;

- The financial institution provides notice of this practice; and
- The financial institution and the third party enter into a contract that requires the third party to maintain the confidentiality of the information and to use the information only as intended.

A financial institution can disclose a consumer's non-public personal information with a non-affiliated entity without providing the consumer the right to opt-out if the information is "necessary to effect, administer or enforce a transaction". In this case, the financial institution does not need to disclose this practice to the consumer.

A financial institution can disclose non-public personal information for compliance purposes (for example, to an insurance rating organisation) and for law enforcement purposes. A financial institution may disclose publicly available financial information (such as publicly available property tax records).

HIPAA does not apply to health information that is not personally identifiable (for example, aggregate data), and it does not apply to health information used by individuals or entities that do not fall within the definitions of "covered entities" or "business associates" of covered entities. For example, some educational and employment records (for example, a report about an individual's fitness for duty that is used to make an employment decision) would not fall within the scope of HIPAA. There are many exemptions from the restrictions on disclosure of PHI, for example, for law enforcement purposes, to avert a serious public health threat, and to facilitate organ and tissue donation.

The disclosure of a security breach required by the California Security Breach Notification Law may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. In addition, a company that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of the law, will be deemed to be in compliance with the notification requirements if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes the information handling procedures of such website.

7. Is notification or registration required before processing data? If so, please provide brief details.

The FTC's Behavioural Advertising Principles suggest that website operators disclose their data collection practices tied to online behavioural advertising and disclose that consumers can opt-out of these practices and provide a mechanism for opting out.

GLB requires a financial institution to provide notice of its privacy practices, but does not have the same notification or registration requirements with a government regulator that exist under the Data Protection Directive.

HIPAA requires a covered entity to provide notice to data subjects of its privacy practices and of data subjects' rights under HIPAA, but does not have the same notification or registration requirements with a government regulator that exist under the Data Protection Directive.

The California Security Breach Notification Law does not have the same notification or registration requirements with a government regulator that exist under the Data Protection Directive. However, in the event of a security breach, notice should be provided in certain circumstances to all affected individuals. Such notice may be provided by one of the following methods:

- Written notice.
- Electronic notice, if the notice provided is consistent with national laws regarding electronic signatures (*15 U.S.C. §7001*).
- Substitute notice, if the company demonstrates that the cost of providing notice would exceed US\$250,000 (about EUR 197,400), or that the affected class of subject persons to be notified exceeds 500,000, or the company does not have sufficient contact information.

Substitute notice must consist of all of the following:

- E-mail notice when the company has an email address for the subject persons.
- Conspicuous posting of the notice on the agency's website page, if the agency maintains one.
- Notification to major state-wide media.

However, if a company maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of the law, the company will be in compliance with the notification requirements if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

The California Online Privacy Protection Act requires commercial websites to disclose their privacy practices, but does not have the same notification or registration requirements with a government regulator that exist under the Data Protection Directive.

MAIN DATA PROTECTION RULES AND PRINCIPLES

8. What are the main obligations imposed on data controllers to ensure that data is processed properly?

The FTC has used section 5 of the FTC Act to charge companies that failed to comply with their own privacy policies. The FTC Act does not expressly require a company to have or disclose a privacy policy, but the FTC's position is that if a company discloses a privacy policy, it must comply with it. In addition, the FTC has stated that it is a violation of the FTC Act for a company to retroactively change its privacy policy without providing data subjects an opportunity to opt-out of the new privacy policy.

GLB seeks to protect consumer financial privacy by limiting when a financial institution can disclose a consumer's non-public personal information to non-affiliated third parties. Financial institutions must notify their customers about their information-sharing practices and tell consumers of their right to opt-out if they do not want their information shared with certain non-affiliated third parties (*see Question 3* for definitions of customer and consumer). Another part of GLB is the Safeguards Rule, which requires companies to develop a written information security plan describing their programme to protect customer records and information. Federal and state agencies with jurisdiction under GLB over financial institutions must implement regulations requiring the financial institutions to establish safeguards under their security programme. Examples include safeguards that:

- Protect against unauthorised access to, or use of, these records or information, which would result in substantial harm or inconvenience to any customer. Common standards that have been suggested to restrict unauthorised access include the use of:
 - data encryption;
 - authentication mechanisms;
 - background checks;
 - frequent monitoring and testing of the information security protocols and systems.
- Ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of these records.
- Implement an Identity Theft Prevention Programme in connection with "covered accounts".
- Implement Response Programme regulations requiring the financial institutions to notify the regulator (and in certain cases the customer) when there has been an unauthorised access to "sensitive customer information".
- Contractually require its service providers to ensure that they are also meeting the objectives of the security programme and monitor them.

In addition, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and re-disclosure of that information.

HIPAA requires (with some exceptions) covered entities:

- To use, request and disclose the minimum amount of PHI necessary to complete a transaction (*HIPAA Privacy Rule*).
- To implement data security procedures, protocols and policies at administrative, technical, physical and organisational levels to protect data (*HIPAA Security Rule*).
- To comply with certain uniform standards established for certain electronic transactions (*HIPAA Transactions Rule*).

The California Security Breach Notification Law is triggered by unauthorised disclosure of unencrypted information so it encourages companies to encrypt the personal information of California residents. Another California statute, Civil Code §1798.81.5, requires certain businesses to use safeguards to ensure the security of Californians' personal information (defined as name plus social security number, driver's license/state ID and financial account number) and to contractually require third parties to do the same. Civil Code §§1798.85-1798.86, 1785.11.1, and 1785.11.6 restrict businesses and state and local agencies from publicly posting or displaying social security numbers and prohibit embedding social security numbers on a card or document using a bar code, chip, magnetic strip or other technology, in place of removing the number as required by law. Civil Code §§1798.80-1798.81 and 1798.84 require businesses to shred, erase or otherwise modify the personal information in records under their control.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes the information handling procedures of such website (see *Question 12*).

9. Is the consent of data subjects required before processing personal data? If so:

- **What rules are there regarding the form and content of consent? Would online consent suffice?**
 - **Are there any special rules regarding the giving of consent by minors?**
-

The FTC's Behavioural Advertising Principles suggest that website operators obtain affirmative express consent (which can be provided online) before using sensitive consumer data. Sensitive data includes (but is not limited to):

- Financial data.
- Data about children.
- Health information.
- Precise geographic location information.
- Social Security numbers.

In addition, website operators that revise their privacy policies should obtain affirmative express consent before using consumer data in ways that are materially different from the privacy policy that was in effect when the data was collected. The FTC also enforces the Children's Online Privacy Protection Act which requires websites that are directed to children, or that knowingly collect personal information from children, to obtain verifiable parental consent before sharing children's personal information.

GLB requires a financial institution, at the time of establishing a customer relationship, and at least annually thereafter, to notify customers and consumers of the institution's privacy policy and practices and allow the individual to opt out of certain disclosures of the individual's non-public personal information. A financial institution must provide the consumer or customer with "reasonable means" to opt out of certain disclosures. Such means can be written, oral or electronic.

HIPAA generally requires covered entities to obtain consent in writing from a data subject before disclosing that data (with certain exceptions, for example, to provide medical treatment). Consent must generally be in writing and contain the signature of the data subject and the date. The HIPAA Privacy Rule provides specific statements that must be included in the consent.

The California Security Breach Notification Law requires disclosure of security breaches, but does not specifically address the requirement for consent. However, other California statutes require express consent when processing personal information, for example, California's medical privacy law (Civil Code §1798.91) prohibits using personal medical information for direct marketing purposes without consent, and California's financial privacy law (Financial Code §§4050-4060) prohibits sharing or selling personally identifiable non-public financial information without consent.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes the information handling procedures of such website, but does not specifically address the requirement for consent.

10. If there is no consent, on what other grounds (if any) can processing be justified?

The FTC Act does not specifically address consent. The Children's Online Privacy Protection Act applies to the online collection of personal information from children under 13, and allows the collection of a child's e-mail address without obtaining parental consent in advance to:

- Provide the required privacy notice and seek consent.
- Respond to a one-time request from a child if the e-mail address is subsequently deleted.
- Respond more than once to a specific request, for example, for a subscription to a newsletter (the operator must notify the parent that it is communicating regularly with the child and give the parent the opportunity to stop the communication before sending or delivering a second communication to a child).
- To protect the safety of a child who is participating on the site.
- Protect the security or liability of the site or to respond to law enforcement.

Under GLB, a financial institution does not need to obtain consent:

- If it shares non-public personal information to administer or enforce a transaction that a customer requests or authorises; or
- If it shares non-public personal information with outside companies that provide essential services, such as data processing or servicing accounts, if certain conditions are met (such as contractual agreements regarding the confidentiality and security of the data). For additional disclosures permitted without obtaining consent, see *Question 6*.

HIPAA generally allows a covered entity to use and disclose PHI without first obtaining consent for “medical treatment”, “payment” or “healthcare operations” (with some exceptions, such as the disclosure of psychotherapy notes). For additional disclosures permitted without obtaining consent, see *Question 6*.

The California Security Breach Notification Law requires disclosure of security breaches, but does not specifically address the requirement for consent.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes the information handling procedures of such website, but does not specifically address the requirement for consent.

11. Do special rules apply in the case of certain types of personal data, for example sensitive data? If so, please provide brief details.

The FTC’s Behavioural Advertising Principles suggest that website operators obtain affirmative express consent before using sensitive consumer data. Sensitive data includes:

- Financial data.
- Data about children.
- Health information.
- Precise geographic location information.
- Social Security numbers.

GLB does not specifically address individual categories of data, however, regulators have also implemented Response Programme regulations requiring the financial institutions to notify the regulator (and in some cases the customer) when there has been an unauthorised access to “sensitive customer information”.

A law relating to GLB, the Fair Credit Reporting Act (15 U.S.C. §1681), limits how consumer reports and credit card account numbers can be used and disclosed. Consumer reports are any communication issued by a consumer reporting agency that relates to a consumer’s credit worthiness, credit history, credit capacity, character, and general reputation that is used to evaluate a consumer’s eligibility for credit or insurance. Financial institutions are prohibited from disclosing an account number to a non-affiliated entity (other than a consumer reporting agency) for telemarketing, email marketing or direct marketing purposes.

Under HIPAA, there are specific rules governing the disclosure of “psychotherapy notes”. In general, a covered entity must obtain written authorisation before disclosing psychotherapy notes, even for purposes of medical treatment, medical operations or payment.

There are several California laws that provide special rules in relation to the processing, collection, transmission and disclosure of certain types of data including:

- Financial and medical data.

- Social security numbers.
- Credit card account numbers.
- Telecommunications records.
- Radio frequency identification (RFID).
- Library records.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

The FTC’s Behavioural Advertising Principles suggest that website operators disclose their data collection practices tied to on-line behavioural advertising and disclose that consumers can opt out of these practices and provide a mechanism for opting out.

GLB requires a financial institution to provide notice of its privacy practices, but the timing and content of this notice depends on whether the data subject is a consumer or a customer. A customer (someone with an established and ongoing relationship with the financial institution) is entitled to receive the financial institution’s privacy notice when the relationship is established and annually thereafter. A consumer (someone who receives a financial product or service, or inquires about one) is entitled to receive the financial institution’s privacy notice if the financial institution intends on sharing the consumer’s non-public personal information. The privacy notice must be a clear, conspicuous, and an accurate statement of the company’s privacy practices. It should describe:

- The categories of information that it collects and discloses
- The categories of affiliated and non-affiliated entities with whom it shares information.
- That the consumer or customer has the right to opt-out of some disclosures (see *Question 6* for details about when an opt-out is required).
- How the consumer/customer can exercise the opt-out right (if an opt-out right is available).

HIPAA requires covered entities to provide a notice of privacy practices to data subjects, generally upon the first visit for treatment. The notice must contain the statement “THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.” The notice must describe:

- The uses and disclosures of PHI the covered entity is entitled to make (such as to receive payment from an insurance company).
- How an individual can access his information.
- How to complain about a HIPAA violation.
- An effective date.

Covered entities are not required to register with a governmental agency, but covered entities must keep records of certain disclosures of PHI.

The California Security Breach Notification Law does not specifically address information that should be provided to data subjects at the point of collection, as it focuses on requirements of disclosure of security breaches.

The privacy policy required under the California Online Privacy Protection Act must:

- Identify the categories of personally identifiable information that the operator collects through the website or online service, and the categories of third-party persons or entities with whom the operator may share that personally identifiable information.
- Explain how a consumer can review his personal information collected by the operator of the website or online service, and how the consumer can make changes to that information, if the website or online service operator allows this.
- Explain how the website or online service operator notifies consumers of changes to its privacy policy.
- State the effective date of the privacy policy.

13. What other specific rights (such as a right of access to personal data or the right to object to processing) are granted to data subjects?

Generally, the FTC Act and most US privacy laws (with the exception of HIPAA and some California laws) do not provide data subjects with specific access rights to their data. However, the Children's Online Privacy Protection Act allows a parent to view the personal information collected by a website about a child, and to delete and correct that information.

GLB allows consumers or customers to opt out of certain disclosures, but generally does not specifically provide access rights to such individuals. However, financial institutions are required, in some cases, to notify the customer when there has been unauthorised access to "sensitive customer information" pertaining to him.

Under HIPAA, a data subject has the right to request access to and to make corrections to his own PHI, and may (with some exceptions) request an account of the manner in which his PHI has been used or disclosed.

The California Shine the Light Law, Civil Code §§1798.83-1798.84, allows consumers to learn how their personal information is shared by companies for marketing purposes and encourages businesses to let their customers opt out of such information sharing. In response to a customer request, a business must provide either:

- A list of the categories of personal information disclosed to other companies for their marketing purposes during the preceding calendar year, with the names and addresses of those companies.

- A privacy statement giving the customer a cost-free opportunity to opt out of such information sharing. Financial services companies subject to the California Financial Information Privacy Act are exempt from this law.

SECURITY REQUIREMENTS

14. What security requirements are imposed in relation to personal data?

The FTC's Behavioural Advertising Principles suggest that website operators that collect and/or store consumer data for behavioural advertising should provide reasonable security for that data and retain data only as long as is necessary to fulfil a legitimate business or law enforcement need. The type of protections afforded to consumer data should be based on the:

- Sensitivity of the data.
- Nature of the company's business operations.
- Types of risk a company faces.
- Reasonable protections available to a company.

The GLB Safeguards Rule issued by the FTC requires companies to develop a written information security plan that describes their programme to protect customer information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. As part of its plan, each company must:

- Designate one or more employees to coordinate its information security program.
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks.
- Design and implement a safeguards programme, and regularly monitor and test it.
- Select service providers that can maintain appropriate safeguards, ensure contracts require them to maintain safeguards, and oversee their handling of customer information.
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The requirements are designed to be flexible. According to the FTC, companies should implement safeguards appropriate to their own circumstances. The FTC's Disposal Rule regulates the destruction of consumer reports. The recently issued Red Flags Rules require financial institutions and creditors to develop a written programme that identifies and detects the relevant warning signs, or "red flags", of identity theft. These can include, for example:

- Unusual account activity.
- Fraud alerts on a consumer report.

- Attempted use of suspicious account application documents.

The programme must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program.

HIPAA requires covered entities to:

- Use and disclose the minimum amount of PHI necessary to complete a transaction.
- Implement data security procedures and policies to protect data.
- Comply with certain standards established for electronic transactions.

There is also Guidance for Remote Use of and Access to Electronic Protected Health Information that specifically addresses the risks associated with storing, accessing and transferring medical data on laptop computers, wireless devices, home computers, flash drives, e-mail and public workstations.

The California Security Breach Notification Law is triggered by the unauthorised disclosure of unencrypted information, so it encourages companies to encrypt the personal information of Californian residents. See *Question 8* for other examples of Californian laws that contain data security requirements.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes the information handling procedures of such website (see *Question 12*).

PROCESSING BY THIRD PARTIES

15. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The FTC has issued several rules, including the Safeguards Rule, the Affiliate Sharing Rule, and the Affiliate Marketing Rule, that limit the sharing and use of financial information and credit report information with affiliates.

Under GLB, a financial institution can disclose an individual's non-public personal information with a non-affiliated entity without providing the individual the right to opt-out if:

- The disclosure is to a third party that uses the information to perform services for the financial institution; and
- The financial institution provides notice of this practice to the individual before sharing the information; and
- The financial institution and the third party enter into a contract that requires the third party to maintain the confidentiality of the information and to use the information only for the prescribed purpose.

HIPAA Privacy Rule permits covered entities to disclose PHI to business associates, if the parties enter into an agreement that requires the business associate to agree to:

- Use the information only for the purposes for which it was engaged by the covered entity.
- Safeguard the information from misuse.
- Assist the covered entity comply with certain of the covered entity's duties under the Privacy Rule.

When a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services Office for Civil Rights.

Under the California Security Breach Notification Law, a third party that maintains computerised data that includes personal information that the third party does not own must notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorised person. California law also provides that a business that discloses personal information about a California resident pursuant to a contract with a non-affiliated third party must require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorised access, destruction, use, modification, or disclosure.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes the information handling procedures of such website, including disclosure of third parties to whom personal information is transferred.

INTERNATIONAL TRANSFER OF DATA

16. What rules govern the transfer of data outside your jurisdiction?

There are very few limits on the transfer of personal data outside the US. Several states have enacted laws that limit or discourage state agencies or state contractors from outsourcing data processing beyond US borders, but these laws are typically limited to state government agencies and private companies that contract to perform services for or provide goods to state agencies.

However, the position of the FTC and other regulators is that US laws and regulations still apply to the data after it leaves the US, and that the regulated entities in the US remain liable for data exported out of the US and remain responsible for the processing of data overseas by subcontractors, and that such entities should utilise the same protections (for example, through the use of security safeguards, protocols, audits and contractual provisions) for the regulated data when it leaves the country.

17. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

For US companies engaging in cross-border transfers of personal data between Europe and the US, there are several options available to effect such transfers in compliance with the Data Protection Directive. The most common methods include, certification under the Safe Harbor program, utilising Commission approved model contracts, or for multinationals, implementing Binding Corporate Rules (BCRs).

The Safe Harbor program was developed by the US Department of Commerce and the Commission to address the Commission's determination that the US does not have in place a regulatory framework that provides adequate protection for personal data transferred from the European Economic Area (EEA). Any US organisation that is subject to the FTC's jurisdiction, and some transportation organisations that are subject to the jurisdiction of the US Department of Transportation, can participate in the Safe Harbor program. Certain industries, such as telecommunication carriers, banks, and insurance companies may not be eligible for this program.

Under the Safe Harbor program, US companies have been able to voluntarily adhere to a set of seven principles:

- Notice.
- Choice.
- Onward transfer.
- Access.
- Security.
- Data integrity.
- Enforcement.

These principles are recognised by the Commission as providing adequate protection and, therefore, meeting the requirements of the Commission concerning transfers of personal data to the US. Participating companies must implement a privacy policy that complies with these principles, and renew their self-certification annually.

Organisations must also be subject to enforcement and dispute resolution proceedings

As an alternative to the Safe Harbor program, US organisations can use standard contractual clauses (model contracts) in their agreements regulating the transfer of personal data from the EEA. The contractual clauses should establish adequate safeguards by creating obligations similar to those in the Safe Harbor program, and incorporate the principles of the Data Protection Directive such as personal data should be collected only for specified, explicit and legitimate purposes. Data subjects should be informed about such purposes and the identity of the data controller. Any person concerned should have a right of access to his data and the opportunity to change or delete data which is incorrect, and appropriate remedies must be available.

US multinationals can also develop a set of BCRs that govern data protection and apply to all intra-group transfers of personal data outside of the EEA. The rules must be approved separately in each EU member state where the multinational has an office, and the applicant must describe its data protection audit plan, the processing and flows of information, the data protection safeguards, and mechanisms for reporting and recording changes, as well as demonstrate that these rules are binding both internally and externally.

Under GLB, before a financial institution transfers any non-public personal information, it must disclose its privacy notice and provide the individual with the opportunity to opt out of certain non-affiliated third party sharing, whether the transfer is within or outside of the US.

The HIPAA Transactions Rule covers "trading partner agreements" involving the exchange of information in electronic transactions. The Department of Health and Human Services has provided sample "business associate agreements", but these are provided as guidance and covered entities are not required to use these sample agreements.

The California Security Breach Notification Law requires the disclosure of security breaches, but does not specifically address the use of data transfer agreements.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes the information handling procedures of such website, but does not specifically address the use of data transfer agreements.

18. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

The FTC's Behavioural Advertising Principles suggest that website operators disclose their data collection practices tied to online behavioural advertising, and disclose that consumers can opt-out of these practices and provide a mechanism for opting out.

GLB requires that a financial institution disclose to a customer its privacy practices and provide the customer an opportunity to opt out of certain disclosures before transferring any non-public personal information. Because the mechanism required is an opt-out provision as opposed to an opt-in, an individual would have to take affirmative action to stop the transfer.

Under HIPAA, if a business associate has signed a business associate agreement that is HIPAA compliant, and the disclosure of PHI is otherwise permitted without obtaining consent from the data subject, the agreement would be generally sufficient to effect the transfer. Trading partner agreements are generally used to address the technology-related obligations of the parties to a transaction and would generally not be sufficient to legitimise a transfer, where authorisation would otherwise be required.

The California Security Breach Notification Law requires disclosure of security breaches, but does not specifically address the use of data transfer agreements.

The California Online Privacy Protection Act requires a commercial website to conspicuously post its privacy policy on its website, which describes the information handling procedures of such website, but does not specifically address the use of data transfer agreements.

19. Does the relevant national regulator need to approve the data transfer agreement? If so, please provide brief details.

Under the US Safe Harbor program and the standard contractual clauses framework, a regulator does not need to approve the data transfer agreement. However if a US multinational wishes to implement the BCRs (see *Question 17*), the rules must be approved separately in each EU member state where the multinational has an office.

GLB does not require a national regulator to approve a data transfer agreement.

HIPAA does not require a national regulator to approve a data transfer agreement, although a regulator may have audit powers to ensure compliance with HIPAA rules.

The California Security Breach Notification Law and the does not specifically address the use of data transfer agreements.

California Online Privacy Protection Act does not specifically address the use of data transfer agreements.

ENFORCEMENT AND SANCTIONS

20. What are the enforcement powers of the national regulator?

The FTC is the primary US enforcer of national privacy laws. Although other national agencies (such as the banking agencies) are authorised to enforce various privacy laws, the FTC brings far more enforcement actions than the other agencies. The FTC can:

- Initiate an investigation.
- Issue a cease and desist order.
- File a complaint in court.

The FTC also reports to Congress on privacy issues and recommends the enactment of required privacy legislation.

GLB is enforced by the FTC, federal banking agencies, and state insurance agencies, although the FTC is more active as an enforcer than the other agencies.

HIPAA is enforced by the Office of Civil Rights within the Department of Health and Human Services. This office can initiate an investigation into a covered entities information handling practises to determine whether it is complying with the HIPAA Privacy Rule, and allows individuals to file complaints about privacy violations.

The California Security Breach Notification Law and the California Online Privacy Protection Act are enforced by the California Attorney General and district attorneys.

THE REGULATORY AUTHORITIES

Federal Trade Commission

W www.ftc.gov

Main areas of responsibility. Broad authority to regulate commercial activities, with particular interest in privacy.

Department of Health and Human Services

W www.hhs.gov

Main areas of responsibility. Oversees enforcement and compliance with HIPAA and the HIPAA Privacy and Safeguards Rules.

California Attorney General

W www.ag.ca.gov,

www.privacy.ca.gov

Main areas of responsibility. Enforcement of California laws.

21. What are the sanctions and remedies for non-compliance with the data protection laws? To what extent are the laws actively enforced?

The FTC Act provides penalties of up to US\$16,000 (about EUR 12,600) per offence. The FTC can also obtain an injunction, provide restitution to consumers, and require repayment of investigation and prosecution costs.

Criminal penalties include imprisonment for up to ten years. In 2006, a data broker agreed to pay US\$15 million (about EUR 11.8 million) to settle charges filed by the FTC for failing to adequately protect the data of millions of consumers. Settlements with government agencies can also include onerous reporting requirements, audits and monitoring by third parties. A major retailer that settled charges of failing to adequately protect customer's credit card numbers agreed to allow comprehensive audits of its data security system for 20 years.

Penalties for violations of GLB are determined by the authorising statute of the agency that brings the enforcement action. For example, an enforcement action brought by the FTC could include penalties of up to US\$16,000 per offence. Individuals who obtain, attempt to obtain, cause to be disclosed or attempt to cause to be disclosed customer information of a financial institution relating to another person through a false, fictitious or fraudulent means, can be subject to fines and/or imprisoned for up to five years. In addition, there are criminal penalties for the perpetrator of up to ten years' imprisonment and fines of up to US\$500,000 (about EUR395,000) (if an individual) and US\$1 million (about EUR790,000) (if a company), if such acts are committed or attempted while violating another US law or as part of a pattern of illegal activity involving more than US\$100,000 (about EUR79,000) in a year.

HIPAA authorises civil penalties of up to US\$25,000 (about EUR19,700) for multiple violations in a calendar year. Criminal

penalties can increase to US\$250,000 (about EUR197,400) and/or up to ten years' imprisonment if the offence was committed under false pretences, or with intent to sell the data for commercial gain.

Some state and federal laws allow individuals to sue for privacy violations, including classes of individuals, and these can also result in significant fines or damages awards. The largest data security breach to date in the US is said to have cost a major retailer at least US\$256 million (about EUR202 million) and perhaps up to US\$500 million (about EUR395 million). The company discovered that credit and debit card numbers of over 45 million consumers were stolen and used to make purchases and open fake accounts. The company settled several class action law suits filed by consumers, as well as law suits filed by credit card companies and banks that had to reissue millions of cards.

The Ponemon Institute calculated that in 2008, the average cost to a US business for each record compromised was US\$202 (about EUR160). In addition to civil and criminal sanctions, se-

curity breaches can have far reaching consequences for companies in terms of loss of customer confidence and trust; customer churn; and loss of revenue, market share, brand and shareholder value.

CONTRIBUTOR DETAILS

Ieuan Jolly

Loeb & Loeb LLP

T +1212 407 4810

F +1646 390 0403

E ijolly@loeb.com

W www.loeb.com

Areas of practice/expertise. Ieuan Jolly advises on international privacy and technology matters with a particular focus on US and pan-European data privacy issues as well as information security risks and mitigation strategies in off-shore jurisdictions such as India.