A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

First Edition

MERITAS®
LAW FIRMS WORLDWIDE

A GLOBAL ROADMAP TO PERSONAL DATA PROTECTION

Asia Pacific, Europe & USA

Dennis Unkovic, Editor

du@muslaw.com
Tel: +1-412-456-2833

Meyer, Unkovic & Scott LLP
www.muslaw.com

Not so long ago, "data protection" meant a locked filing cabinet and a good shredder. No longer. In a single generation, protecting data went from safeguarding documents to securing information of almost every kind, both tangible and in electronic form. Although everyone understands what it means to protect a hard copy document, it is much harder to conceptualize protecting intangible information. To make matters worse, a data breach today can cause far more serious consequences than in years past. To cite just one example, the improper disclosure of one's personal data can easily result in identity theft, with the victim often left unaware of the crime until it is far too late to stop it.

With the endless march of technology and an increasingly connected world, protecting personal data is clearly more important than ever. In response, governments around the world have focused on enacting legislation to keep up with the fast pace of change. The EU's recent implementation of the General Data Protection Regulation (GDPR) is just the latest development in this crucial area of law. Outside the EU, however, there is little uniformity in how different regions and countries protect personal data. To help make sense of this, Meritas® has produced this guide by leveraging its top quality member firms from around the world, specifically our firms in Asia Pacific, Europe and the USA. The guide employs a straightforward question-and-answer format to be as simple and as easy to use as possible. The authors hope that this guide will provide readers with a convenient and practical starting point to understand a complicated yet vitally important subject to businesses everywhere.

Special thanks go out to Meritas® Board Member Yao Rao (China), who was the inspiration behind this publication, as well as to Meritas® Board Member Darcy Kishida (Japan) and Eliza Tan (Meritas® Asia Regional Representative), who provided crucial support. Without their hard work and dedication, this global look at the critical issue of Data Privacy would not have been published.

ABOUT MERITAS®

Founded in 1990, Meritas® is the premier global alliance of independent law firms working collaboratively to provide businesses with qualified legal expertise. Our market-leading member firms offer a full range of high-quality, specialized legal services, allowing you to confidently conduct business anywhere in the world.

As an invitation-only alliance, Meritas® firms must adhere to our uncompromising service standards to retain membership status. Unlike any other network or law firm, Meritas® collects peer-driven reviews for each referral, and has for more than 25 years.

7,500+ EXPERIENCED LAWYERS

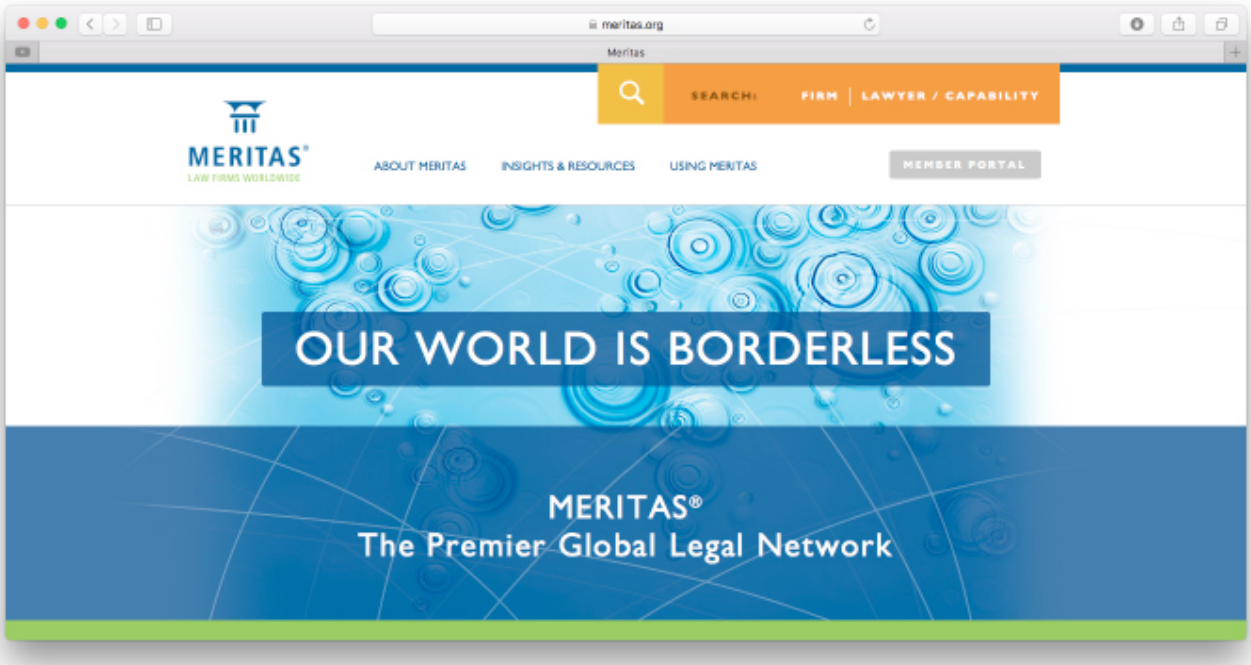
90+ COUNTRIES

180+ LAW FIRMS

240+ GLOBAL MARKETS

Using this exclusive ongoing review process, Meritas® ensures quality, consistency and client satisfaction.

With 180+ top-ranking law firms spanning more than 90 countries, Meritas® delivers exceptional legal knowledge, personal attention and proven value to clients worldwide.



For more information visit:

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

MERITAS®
LAW FIRMS WORLDWIDE

USA

FIRM PROFILE:

MEYER UNKOVIC SCOTT
ATTORNEYS AT LAW

Meyer, Unkovic & Scott established in 1943 is a full service law firm with a diverse clientele including Fortune 100 companies, significant financial institutions, business enterprises, and individuals. Our firm has extensive experience handling international matters for its clients across the globe.

We advise on legal matters, including structuring a variety of business transactions, mergers & acquisitions, foreign direct investments, intellectual property and data protection, real estate and banking law, insolvency law, employment law, international law, immigration issues, tax planning, and commercial litigation and arbitration.

We strive to understand each client's unique goals and needs. Our most important priority is clear, concise, and regular communications.

Dennis Unkovic served as the world-wide Chair of Meritas® from April 2015 to May 2018. Meyer, Unkovic & Scott has been an active member of Meritas® since October 11, 1999.

CONTACT:

DENNIS UNKOVIC
du@muslaw.com

MICHAEL G. MONYOK
mgm@muslaw.com

+1-011-412-456-2800
www.muslaw.com

Introduction

Data privacy is an important and evolving issue in the United States. Various national and state-level laws and regulations protect the collection, storage, and use of personal information. At the national level, there are several federal agencies charged with the enforcement of applicable laws and regulations, including the Federal Trade Commission (the "FTC"), the Department of Health and Human Services (the "DHS"), and the Consumer Financial Protection Bureau (the "CFPB"). The distributed enforcement duties among various agencies results from the lack of a single, comprehensive law relating to the protection of personal information.

1. What are the major personal information protection laws or regulations in your jurisdiction?

The following is an overview of the current law and regulations of most concern to businesses operating in the US:

(1) Federal Trade Commission Act (15 USC §§ 41-58): Provides general authority to the FTC to regulate deceptive and unfair trade practices. The FTC has interpreted its charter to include the authority to regulate cybersecurity practices and the unauthorized disclosure of personal information. A federal court has confirmed the FTC's authority in an enforcement proceeding brought by the FTC against Wyndham Hotels. The FTC initiated the enforcement proceeding, alleging that Wyndham Hotels unfairly exposed the payment card information of hundreds of thousands of guests to hackers in three separate breaches by failing to implement a reasonable security program. Wyndham Hotels paid a significant fine to settle the suit.

(2) HIPAA Regulations (45 CFR 160): This Rule regulates the collection and use of protected health information by hospitals, healthcare providers, doctors, healthcare clearinghouses, and any business associate of the foregoing.

(3) Children's Online Privacy Protection Rule (FTC Regulation 16 CFR 312): This rule prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the internet. Under this rule, parents have control over what information can be collected about their child.

(4) Privacy of Consumer Financial Information (FTC Regulations 16 CFR 313): Pursuant to this section of the FTC regulations, financial institutions are required to provide notice to customers about their privacy policies and practices. In addition, the rules describe situations where a financial institution may disclose nonpublic personal information about customers to nonaffiliated third parties.

(5) Standards for Safeguarding Customer Information (FTC Regulations 16 CFR 314): Entities that are subject to FTC regulations "shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards" to protect the security, confidentiality, and integrity of customer information. Covered entities include financial institutions, which is broadly defined, and any service provider to a covered entity.

(6) CAN-SPAM Rule (FTC Regulations (16 CFR 316): Regulates the collection and use of email addresses.

(7) Electronic Communications Privacy Act (15 USC § 2510) and Computer Fraud Abuse Act (18 USC § 1030): These laws restrict the intercept of electronic data, whether in transmission or stored, and prohibits access to a computer without authorization.

(8) State Privacy Laws: Nearly all 50 states have laws requiring notification to an individual whose personal information was involved in a security breach.

2. How is personal information defined?

The definition of personal information will vary depending on the particular law or regulation

being applied. In general, the term typically relates to information that can be used to identify an individual, whether alone or in combination with other pieces of information. For example, the FTC considers a person's name, address, social security number, credit card number, account information, and other similar data as "personally identifiable information." Many states take a similarly open-ended approach, where a person's name or additional piece of information that could be used to identify a person is considered personal information. The HIPAA Regulations apply to any "individually identifiable health information", stored in any form, whether, electronic, paper, or oral. The laws and regulations typically reference "customers" or "individuals", so the protections afforded to personal information likely applies to citizens and non-citizens alike. In addition, many of the regulations aim to protect data associated with an individual, rather than a corporation.

3. What are the key principles relating to personal information protection?

The key principles in relating to personal information protection in the United States are: (1) Creating and following a privacy policy for the collection and use of information from customers; (2) Using reasonable safeguards for the protection of personal or sensitive information; and (3) Providing notice of a breach to every individual whose information has been compromised.

While the term "reasonable" can be ambiguous, federal agencies in the United States have adopted as official policy the Cybersecurity Framework ("Framework"; available at <https://www.nist.gov/cyberframework>) created by the National Institute of Standards and Technology, a federal agency that promotes innovation and industrial competitiveness. The Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risks. Adherence to the Framework satisfies the "reasonableness" standard used by the FTC in determining whether a company's activities are deceptive or unfair and also satisfies the HIPAA requirements. For example, in an enforcement action brought by the FTC, it alleged that Petco Animal Supplies, a large national retail chain, failed to implement policies and procedures to safeguard consumers' information. Establishing an organizational information security policy, as suggested in the Framework, would have addressed this issue.

4. What are the compliance requirements for the collection of personal information?

Collection of personal information is generally not subject to regulation. In this regard, Europe is far ahead of the United States in regulating the collection of personal information with the implementation of the General Data Protection Regulation. Although not a requirement, the FTC, in its self-regulatory principles for online behavioral advertising, suggests that websites disclose their data collection practices and provide a customer the ability to opt-out.

5. What are the compliance requirements for the processing, use and disclosure of personal information?

As noted above, the compliance requirements for the processing, use, and disclosure of personal information is dependent on which law or regulation applies. Except for most health or some financial information, the processing, use and disclosure of personal information is not prohibited. With respect to health and financial information, an entity can disclose such information only as permitted in the regulations. For example, a doctor can transmit health information to an insurance company. To ensure the security of information transmitted in these situations, the entity is usually required to have a contractual relationship with the receiving party in which the receiving party agrees to be bound to the same security requirements as the disclosing party.

6. Are there any restrictions on personal information being transferred to other jurisdictions?

There are few restrictions on the transfer of personal information to foreign jurisdictions. However, an entity may still be subject to FTC authority for activities that

involve information transferred outside of the US. For example, Facebook is being probed by the FTC for allowing a consulting firm in the UK to access the profiles of millions of US-based Facebook users. Facebook's actions have also subjected it to investigations led by the attorneys general of New York and Massachusetts.

7. What are the rights of an individual whose personal information is collected? Can he/she withdraw the consent to the retention of his/her personal information by a third party, and if so, how?

An individual does not have specific rights to their information. Further, since consent is not required for the retention of information, an individual cannot withdraw consent. Notwithstanding the foregoing, a parent has certain rights to information about their child under the Children's Online Privacy Protection Act. In addition, if an individual's personal information is used fraudulently, that individual may have recourse against the person or entity that misused or leaked the data. The fraudulent actor may also be subject to criminal penalties.

8. Is an employee's personal information protected differently? If so, what's the difference? Apart from the personal information of employees, are there any other types of personal information that receive special protection?

An employee's personal information is generally not treated differently under federal law or state law. Although, an employer cannot engage in discriminatory hiring practices based on information collected or made available to the employer, such as a person's medical history, family status, race, or religion. If this occurs, the individual who is denied employment would have a cause of action against the employer. In addition, as previously noted, financial and health information is treated differently than general personal information in terms of how the information can be disclosed or shared.

9. Which regulatory authorities are responsible for implementation and enforcement of personal information protection laws in your jurisdiction?

The FTC, DHS (related to HIPAA regulations), and the CFPB are the main federal agencies responsible for the enforcement of personal information protection laws in the US. In addition, various state agencies are responsible for state-level laws and regulations related to personal information.

10. Are there any penalties, liabilities or remedies if any of the personal information protection laws is violated?

Violation of laws and regulations related to personal information can result in fines from government agencies, civil lawsuits brought by individuals whose information was misused, and liabilities that are merely related to the data breach. As an example of a penalty resulting from an enforcement action brought by the FTC, LifeLock (a company who provides identity protection services, ironically) agreed to pay a $100 million fine for failing to secure consumers' personal information. The large size of the fine resulted because LifeLock violated a previous court order requiring it to implement such practices and failed to keep records of its efforts to protect its customers' data.

As an example of how a data breach can lead to liabilities that extend beyond the damages caused by the breach itself, the Securities and Exchange Commission (the "SEC") recently fined Yahoo $35 million for failing to disclose to investors a data breach involving the unauthorized access to hundreds of millions of user accounts, which included the usernames, email addresses, passwords, birthdates, phone numbers, and answers to security questions. Given the extent of the breach, the SEC determined that Yahoo misled investors since the breach was likely to have significant financial and legal implications.

11. Is your jurisdiction planning to pass any new legislation to protect personal information? How

is the area of personal information protection expected to develop in your jurisdiction?

In response to recent breaches involving the unauthorized disclosure of personal information, the United States Congress has proposed legislation that would provide individuals with greater control over their personal information. For example, the Social Media Privacy Protection and Consumer Rights Act of 2018 would require operators of websites to provide users a copy of the data that has been collected about them. Under the proposed legislation, the website operators would also be required to provide details on how the data is being used by the website, to indicate if it has been made available to third parties, and to notify users within 72 hours if their data has been misused in any manner.

Similarly, the state of California has recently enacted the California Consumer Privacy Act, which requires websites to show users the data that is collected about them, how the data will be used, and to identify third parties that will have access to the data. The law does not take effect until 2020 and is receiving criticism from many technology companies, so the data privacy law may change before it is implemented.

Conclusion

As discussed above, the US Congress has proposed legislation protecting user's information collected by website operators. The legislation is one of many currently being considered. Further, US regulations, which are implemented by a particular agency and do not require additional authorization from Congress, continue to evolve as the type of data and the nature of its use continues to change. Even if regulations did not evolve, enforcement actions brought by the FTC and other agencies continue to help define acts that are considered "unlawful" under existing laws and regulations. As a result of the divided enforcement responsibilities, lack of unification, and changing legislative and enforcement landscape, those operating in the United States would benefit from staying abreast of the current standards for protecting personal information.

Author: Michael Monyok

Prepared by Meritas Law Firms

Meritas is an established alliance of 180+ full-service law firms serving over 240 markets – all rigorously qualified, independent and collaborative. Connect with a Meritas law firm and benefit from local insight, local rates and world-class service.

www.meritas.org enables direct access to Meritas law firms through a searchable database of lawyer skills and experience.

MERITAS®
LAW FIRMS WORLDWIDE

www.meritas.org

800 Hennepin Avenue, Suite 600
Minneapolis, Minnesota 55403 USA
+1.612.339.8680