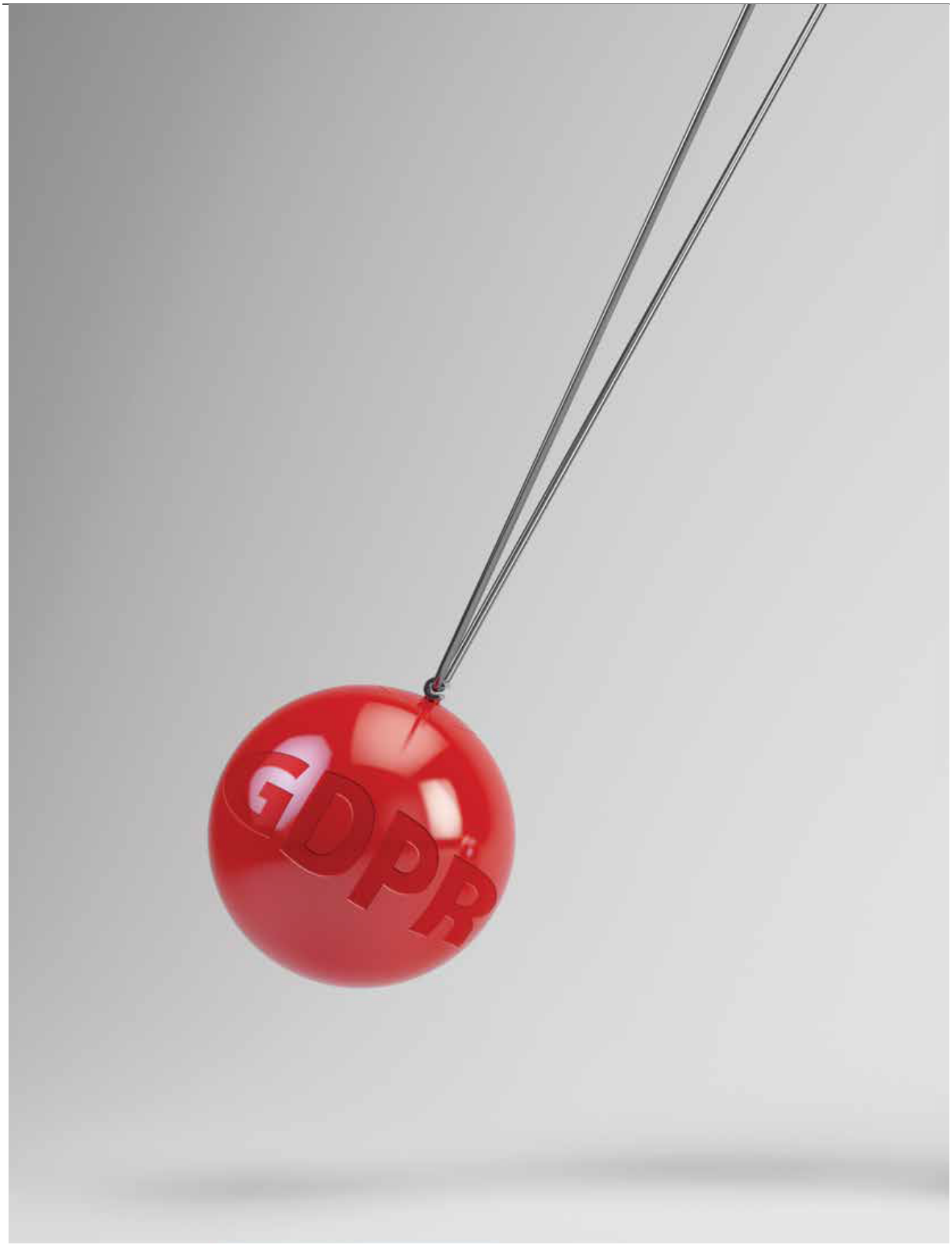
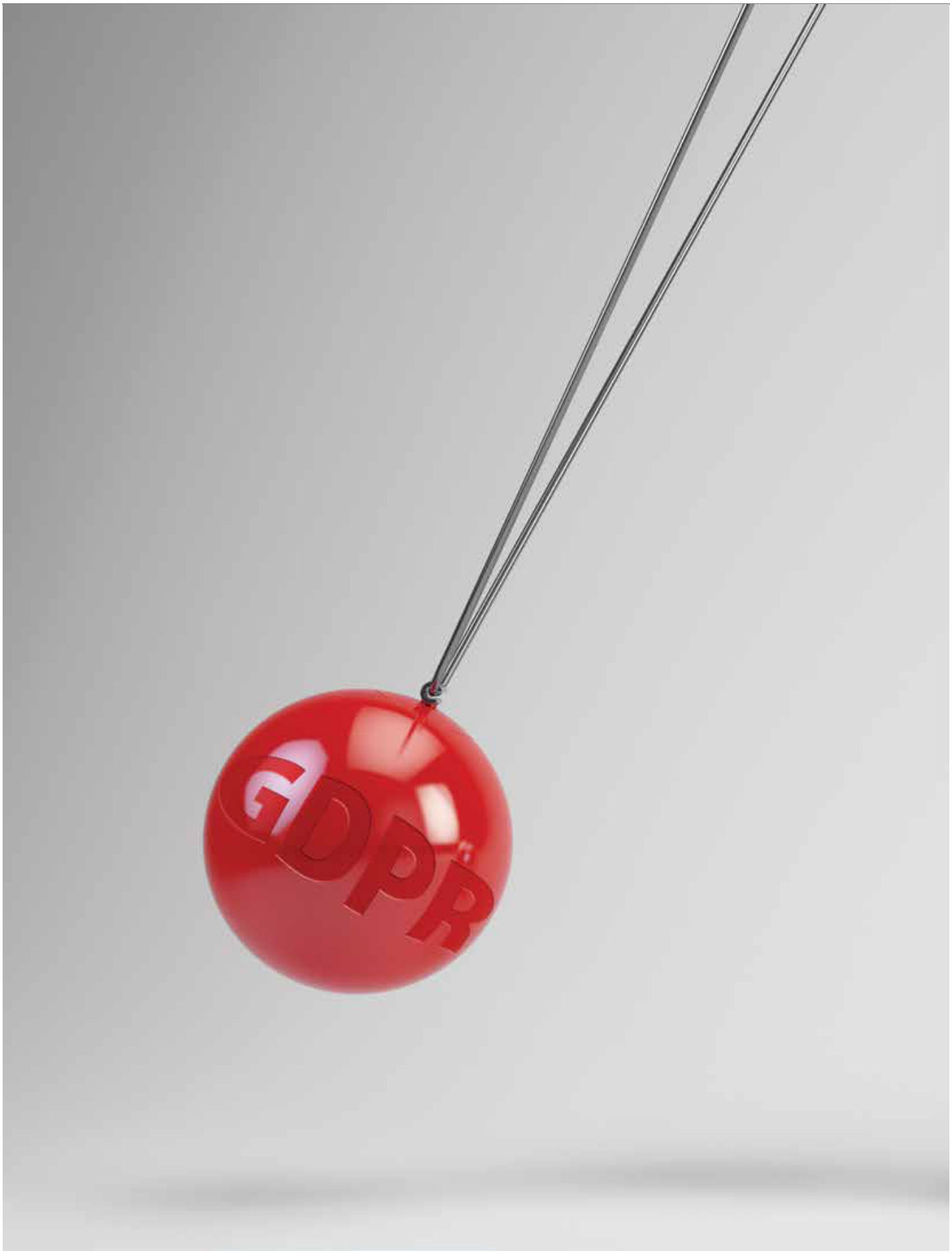
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Impact of Emerging Models of Data Privacy Laws in Europe and the United States

Compliance and Ethics

Technology, Privacy, and eCommerce


GDPR


GDPR

CHEAT SHEET

- ***Out with the old.*** The European Union plans to replace its outdated EU Privacy Directive with the General Data Production Regulation, which will have a stronger international presence.
- ***Expanding reach.*** US privacy laws are changing to provide the Federal Trade Commission with more authority to establish comprehensive information programs that better protect the consumer.
- ***Behind the shield.*** In an effort to replace the US Safe Harbor Program, the European Commission announced the EU/US Privacy Shield, which will enforce the lawful transfer of personal data to and from the European Union.
- ***Protect and monitor.*** Once you have a firm idea of where your company is likely to head in the future, keep track of changing privacy laws and evaluate whether you have the adequate personnel and resources to accommodate them.

As in-house counsel, we are often responsible for the difficult task of anticipating trends regarding how the legal and regulatory landscape is likely to change so we can help our companies stay ahead of the curve. The sooner we can detect the trend — the better. That way, we can marshal sufficient time and resources to prepare and implement compliance measures.

New data privacy laws in Europe and the United States are expected to have a notable impact on many multinational companies. Historically, the United States and the European Union have had very different data privacy standards, but now their models are heading in the same general direction. Companies will want to stay ahead of this trend, as the new direction of data privacy will portend higher regulations and compliance requirements.

The historical European model of data privacy regulation

Europe’s data privacy model relies on a comprehensive approach. Laws are passed at the national level, which regulates many sectors of the entire country. For example, in 1995, the European Union passed a Data Protection Directive (Directive) that required the protection of personal data. The Directive is a legal act of the European Union, which requires member states to achieve a particular result without dictating the means of achieving that result. As I will discuss later, there is a lot of change occurring with regard to EU data protection laws. Still, this background is helpful because the Directive provides a good baseline to begin to see the regulatory trend that is emerging.

The Directive is very broad. It applies to any information relating to an identified person or information that can be used to identify a person, e.g., a list of salaries along with employee ID numbers. On the other hand, these laws do not apply to truly anonymous data that cannot be used to obtain a person’s identity.

Companies in Europe must comply with detailed requirements when collecting, using, and storing personal data, including but not limited to:

- The personal identifiable data must be used fairly and lawfully;
- Process and store personal identifiable data for specific, lawful purposes;
- Ensure that the personal identifiable data is accurate and any errors corrected;
- Maintain the personal identifiable data no longer than necessary for the legitimate purpose which it was collected; and,
- Ensure that adequate security measures protect the personal identifiable data.

The EU Directive is so broad that it often regulates companies in the United States. A company in the European Union may wish to transfer its personal data overseas, so that people outside of the European Union can have access to it. For example, an EU company may wish to transfer employee or customer data to its US affiliate, or transfer personal data to its business partner or customer in the United States.

However, according to the Directive, a company in the European Union can transfer personal data outside of Europe only if there is an “adequate level of protection” in place to protect the personal data. This generally means that the non-EU country must be in compliance with European data privacy laws.

The European Union has recognized that some countries have an adequate level of protection to lawfully permit the transfer of EU personal data. These fortunate countries are Andorra, Argentina, Canada (commercial organizations), Faeroe Islands, Guernsey, Israel, the Isle of Man, Jersey, New Zealand, Switzerland, and Uruguay.

As you can see, the United States is not a part of the fortunate few. However, there are other means for countries like the United States to lawfully transfer personal information to and from the European Union. Previously, one of the alternative means available only to the United States was the Safe Harbor program. Safe Harbor was a program agreed upon by the European Union and the United States that allowed US companies to self-certify that they would comply with EU data protection standards. Typically, as part of the self-certification process, the US company would implement internal measures to protect European personal data. For example, many companies would implement a data privacy policy by training its employees on data protection, and conducting a regular audit. The US company would then file a certification with the US Department of Commerce to participate in the Safe Harbor program. Once the US Department of Commerce approved the certification, the US company could lawfully receive EU personal data.

The historical US model of data privacy regulation

Unlike the European Union, the United States uses a sectoral approach. There is no single comprehensive data privacy law that regulates all personal information. Laws are enacted to regulate a particular industry. For example, the Health Insurance Portability and Accountability Act (HIPAA) regulates medical privacy. The Gramm-Leach-Bliley Act requires financial institutions to safeguard sensitive data. The Children’s Online Privacy Protection Act protects the personal information of children under the age of 13.

The reason for the different models of data privacy regulation

The differences in the US and EU models of data privacy regulations are due to historical and cultural differences. Europe has had recent experiences with centralized authoritarian governments that abused personal privacy, e.g., fascism and communism. For example, a *New York Times* article

discussed the US National Security Agency's monitoring of the personal cell phone of Angela Merkel, the chancellor of Germany. This article stated that:

> "In an angry conversation with Mr. Obama in October after the phone monitoring was revealed, Ms. Merkel said that the NSA's activities reminded her of growing up as the daughter of a Protestant minister in East Germany. She told him, 'This is like the Stasi.'"

The Stasi was the all-powerful secret police of former communist East Germany that violated the personal privacy of its citizens.

On the other hand, the United States has not experienced this sort of extreme centralized authoritarian government. Traditionally, the United States has a less accepting attitude toward central authority than in Europe. Think of the American Revolution, which led to severed ties between the colonists and the English authoritarian central monarchy. More recently, there have been many critics of the US federal government and over-regulation, as exemplified by former US President Ronald Reagan's inaugural address delivered in Washington, DC on January 20, 1981:

> "In this present crisis, government is not the solution to our problem; government is the problem. From time to time, we have been tempted to believe that society has become too complex to be managed by self-rule, that government by an elite group is superior to government for, by, and of the people . . . We are a nation that has a government — not the other way around. And this makes us special among the nations of the Earth. Our government has no power except that granted it by the people. It is time to check and reverse the growth of government which shows signs of having grown beyond the consent of the governed . . . It is no coincidence that our present troubles parallel and are proportionate to the intervention and intrusion in our lives that result from unnecessary and excessive growth of government."

The emerging trend of the US and EU models of data privacy regulation

The emerging trend is that the European Union and the United States are taking a stronger stance on data privacy regulation. However, there are still significant differences between the United States and the European Union, and this gap will likely remain due to their historical and cultural differences. Thus, if your business has greater focus on the European Union than the United States, you will likely need to consider allocating greater time and resources for data privacy compliance.

European Union

The European Union plans to replace its Directive with an even stronger set of regulations. Recently, the European Parliament and the Council of the European Union announced sweeping new EU data protection regulations known as the General Data Protection Regulations (GDPR). Enforcement of the GDPR commences on May 25, 2018. Although many of the core concepts remain the same, the GDPR has a much broader and stronger reach than previous regulations. For example, the GDPR applies to companies outside of the European Union that process EU personal information in the offering of goods and services to people in the European Union. Enforcement powers such as fines have also increased.

The GDPR requires that any non-EU company have an adequate level of protection in place before EU personal information can be transferred outside of the European Union. However, under new regulations, the Safe Harbor program is no longer valid. In October 2015, the European Court of Justice invalidated the Safe Harbor program, stating that it did not provide an adequate measure of protection when transferring EU personal information to the United States.

Recently, the European Commission announced the new EU/US Privacy Shield program, which is meant to replace the US Safe Harbor Program. Like the Safe Harbor program, the Privacy Shield is a voluntary, optional means for an US company to have an adequate level of protection in place to permit the lawful transfer of EU personal data. The intent of the Privacy Shield program is to strengthen data privacy regulation. As stated by a commissioner in a European Commission press release:

> "The EU-US Privacy Shield is a robust new system to protect the personal data of Europeans and ensure legal certainty for businesses. It brings stronger data protection standards that are better enforced, safeguards on government access, and easier redress for individuals in case of complaints. . . ." [emphasis added]
>
> European Commission Press release, "European Commission launches EUU. S. Privacy Shield: stronger protection for transatlantic data flows," Brussels, July 12, 2016.

The Privacy Shield, however, holds US companies to a higher standard than the Safe Harbor program. For example, unlike the Safe Harbor program, the US Department of Commerce will need to conduct regular updates and reviews of participating companies to ensure compliance.

United States

The US data privacy laws are also changing. Due to concerns about privacy arising from data breaches, the United States is heading toward stronger regulation. However, in the near future, US regulations are unlikely to be as comprehensive as those in the European Union due to cultural and historical differences discussed earlier. For example, the Federal Trade Commission (FTC) has emerged to become the national data privacy enforcer regarding e-commerce. Since e-commerce is continually growing in importance, US companies should increasingly monitor the FTC and its developing data privacy authority.

Why the FTC? At first blush, it is a bit unusual to think of the FTC as a data privacy regulator. Hence, it is worthwhile to analyze how the FTC has historically evolved into this role.

The FTC's mission is to protect consumers. Its key enforcement mechanism is section five of the FTC Act which prohibits "unfair or deceptive acts or practices in or affecting commerce." The FTC can investigate a claim that a company has committed an unfair or deceptive practice. After the investigation, the FTC can issue a complaint for trial before an administrative law judge. The decision can be appealed to the FTC commissioners and then ultimately to a federal district court. In practice, FTC enforcement actions are usually settled through consent decrees in which the respondent does not admit fault but agrees to change its practices.

In the 1990s, commercial activity on the internet greatly increased. As e-commerce has evolved to a great degree in the United States, the FTC enforcement of e-commerce has evolved as well. For example, it became common practice for companies to post privacy notices on their commercial website. These privacy notices informed consumers about how their personal information was being

collected and used.

In 1998, the FTC settled its first internet privacy enforcement action brought against GeoCities. GeoCities operated a website that provided an online community through which users could maintain personal homepages. Geocities collected personal information and promised on its website that the personal information would not be sold or distributed without consent. In this case, the case settled after the FTC alleged that Geocities engaged in a deceptive practice by, for example, disclosing the personal information to third parties without consent. Geocities agreed to post and adhere to a privacy notice that correctly disclosed to users how it collects and uses personal information.

In 2002, the FTC settled an enforcement action brought against Eli Lilly. Eli Lilly maintained a website that promised the security and privacy of a given user's personal information. After a breach of such data, the FTC brought and settled an enforcement action that required Eli Lilly to develop and maintain an information privacy and security program to protect consumer privacy in the future.

A few months later, the FTC settled an action brought against Microsoft for making misleading representations about the security of personal information collected through its "Passport" website service. Under the settlement terms, Microsoft agreed not only to implement a comprehensive security program, but also elected to undergo a third party audit to ensure compliance with such a security program every two years.

It has become quite common for the FTC to require the implementation of a comprehensive security program, which typically includes audits by third parties. For example, in a recent decision finding against LabMD in July 2016, the FTC ordered the company to establish a comprehensive information security program to "obtain periodic independent, third party assessments regarding the implementation of the information security program."

Is this expansion of the FTC data privacy enforcement legally invalid? Has the FTC overstepped its legal authority? Recently, the Third Circuit Court of Appeals passed upon the FTC's legal authority to regulate data privacy and affirm FTC practices. In 2012, the FTC filed a complaint against Wyndham, alleging that the company had engaged in unfair and deceptive cybersecurity, which resulted in a data breach of consumer's personal information. Unlike previous companies, Wyndham refused to settle and challenged the FTC's legal authority in federal court. Wyndham argued that the FTC's enforcement activity had exceeded its regulatory authority.

On August 24, 2015, the Third Circuit Court of Appeals rejected Wyndham's arguments, thereby strengthening the FTC's authority to engage in its enforcement actions. The court's opinion may be an indicator of judicial acceptance of increased data privacy regulation:

> "A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business."
>
> *Federal Trade Commission v. Wyndham Worldwide Corporation*, 799 F.3d 236, 245 (3rd Cir. 2015).

On December 9, 2015, the FTC announced a settlement with Wyndham, which required the establishment of an information security program, as well as annual information security audits.

Conclusion

Prudent in-house counsels seek to stay ahead of legal trends to better allocate time and resources. Now is the time for in-house counsel to begin considering the emerging trend of greater data privacy regulations in the European Union and United States.

Speak to your business partners and learn as much as you can about the future of conducting business in Europe and/or e-commerce in the United States. Once you have a firm idea as to where your company is likely to head in the future, keep track of changing data privacy laws and consider whether you have the adequate personnel and resources to meet new standards. If not, then consider the additional personnel and resources needed and develop a plan to obtain approval from management. Finally, as your company's business plan evolves, ensure that your compliance with data privacy law evolves with it.

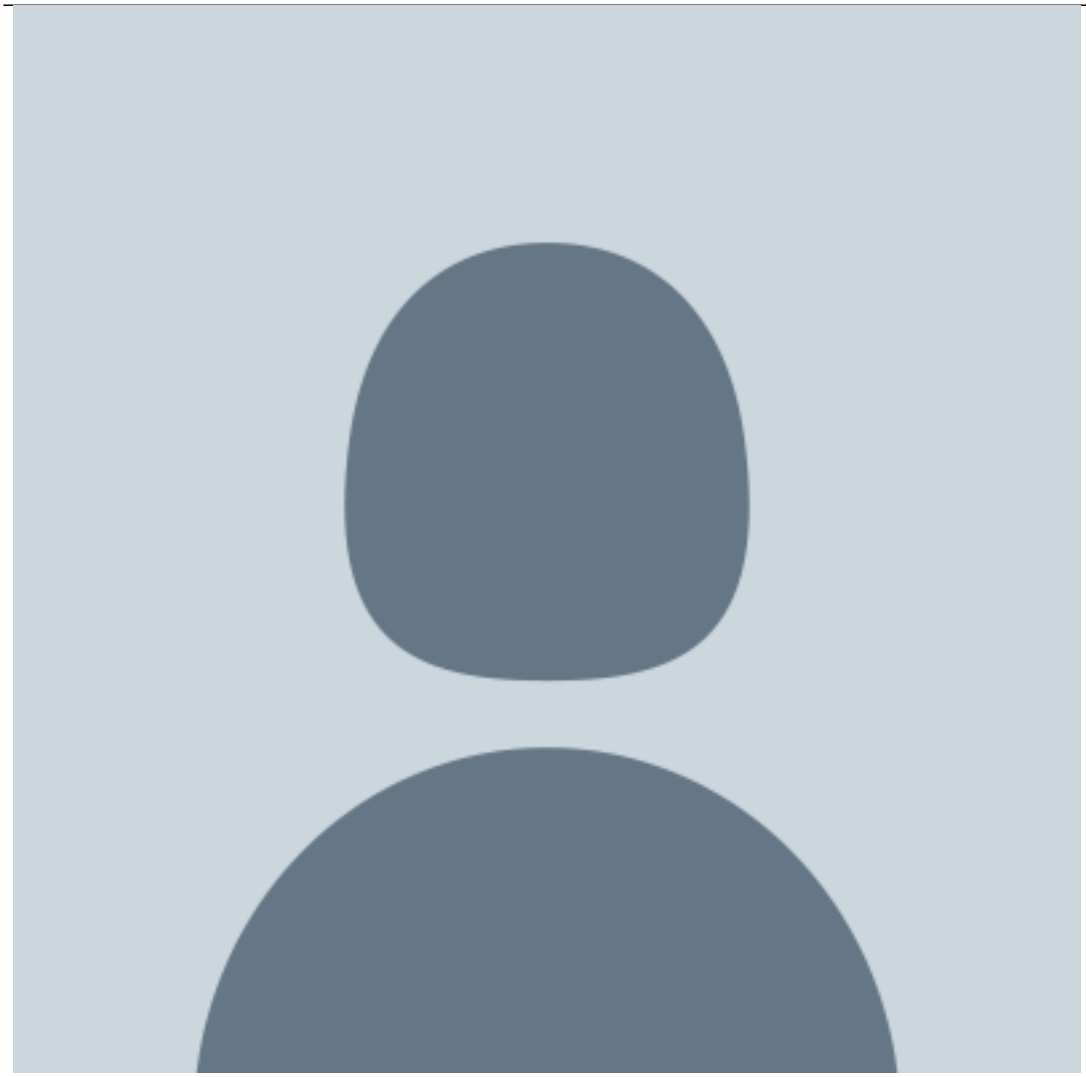
Further Reading

EU Directive 95/46/EC.

The law firm of Hunton & Williams has created a good overview comparing the Directive and GDPR titled "The EU General Data Protection Regulation: A guide for in-house lawyers," April 2016.

Maximillian Schrems v Data Protection Commissioner, case C 362/14, Court of Justice of the European Union, October 6, 2015.

David B. Kahng



Global Human Resources Attorney

The Nature Conservancy in Arlington, Virginia

He works primarily on data privacy and labor and employment matters.