KEEPING UP WITH FAST-CHANGING INTERNATIONAL PRIVACY LEGISLATION

BY
DR. JESSICA SANTOS

JANUARY 2019
Since the beginning of the millennium, the global privacy landscape has undergone dramatic changes. In one regard, data is now viewed as an asset, commodity or even a hard currency that organizations must possess\(^1\); while in another regard, data subjects and regulators are placing increasing demands on data privacy that organizations must adhere to in order to avoid personal data violations.

Considering that there’s no universal consistency on the principles of data protection or how personal data is handled, differences of how privacy is interpreted is largely based on the founding principles of individual countries and regions, which drives legislation and thus enforcement actions.

THE GLOBAL PRIVACY LANDSCAPE - 2001 VS. 2018

Ref: Data Protection Laws of the World, DLA Piper\(^2\)
THE PRINCIPLE OF PRIVACY

What is the principle of privacy? Is it a human right, a commodity, or a secondary consideration to the interests of states?

In fact, all three of these broad categories define the interpretation of privacy:

1. PRIVACY IS A HUMAN RIGHT

In the EU, human dignity is recognized as an absolute, fundamental right. Considering this notion, privacy – or the right to a private life, to be autonomous, to be in control of information about one’s self, to be let alone – plays a pivotal role in EU privacy legislation. That’s because privacy is viewed as not only an individual right, but also a social value.3

The EU’s new General Data Protection Regulation (GDPR) states that EU citizens’ personal data can only be transferred to countries with an “adequate” data protection status. The European Commission (EC) says that countries such as Andorra, Argentina, Canada, Switzerland, Faroe Islands, Jersey, Japan, New Zealand, Guernsey, Israel, Isle of Man and Uruguay share in the EU’s principles that privacy is a human right.

Moreover, almost every country in the world recognizes privacy in some way, be it in their constitution or in other provisions. Nonetheless, even though privacy is recognized as a universal human right, data protection is not – at least not yet.

The right to privacy or a private life is enshrined in the United Nations’ Universal Declaration of Human Rights (Article 12)4, the European Convention of Human Rights (Article 8)5; and the European Charter of Fundamental Rights (Article 7)6.

Perhaps the most recognized piece of legislation is the EU’s 2018 GDPR, which is designed to give citizens more control over their own private information in a digitized world of smartphones, social media, Internet banking, remote data collection and processing, and global transfers. The GDPR also sets minimum standards for the use of data for policing and judicial purposes.

These actions are of no surprise, since Europeans, after all, have consistently shown a significantly lower tolerance for privacy invasion than Americans. This, perhaps, can be attributed to Europeans’ experiences with various all-knowing, totalitarian regimes in the last century.7

2. PRIVACY CAN BE A COMMODITY

Historically, in some parts of the world, such as the United States, privacy has often been regarded as an element of liberty – the right to be free from intrusions by the state. This privacy distinction is relative in other parts of the world since it’s also an element of privacy in the EU.

The supreme law in the United States is the U.S. Constitution, drafted originally at the Constitutional Convention of 1787.8 While the U.S. Constitution does not contain the word “privacy”9, the right to privacy is most often protected by statutory law. For example, the Health Information Portability and Accountability Act (HIPAA)10 protects a person’s health information, while the Children’s Online Privacy Protection Act (COPPA)11, the Gramm-Leach-Bliley Act (GLBA)12 and the Federal Trade Commission (FTC) enforce the right to privacy through various privacy policies and statements.
In the United States, it’s common to refer to data as “assets”, which can be sold, purchased or transferred from one entity to another with a price tag, especially in the era of Big Data. Data is often listed as a business asset in corporate balance sheets, Master Service Agreements (MSAs) and in merger and acquisition deals.

Nonetheless, the right to privacy must be balanced against the state’s compelling interests, including the promotion of public safety and the improvement of quality-of-life. Seat-belt laws and motorcycle helmet requirements are examples of such laws. Many Americans are well aware that their government collects personal information, however, most say that government surveillance is acceptable.

3. PRIVACY IS SECONDARY TO STATE INTERESTS

Many countries, such as Russia and People’s Republic of China (PRC), have the protection of “national interest” in their constitutions. This has created an ongoing conflict with personal privacy, and a trade-off or compromise is not easily balanced.

This is contrary to U.S. law. For example, in a well publicized case in early 2016, Apple CEO Tim Cook refused to cooperate with the U.S. government to unlock the iPhone used by Syed Farook, one of the two perpetrators in the San Bernardino, California mass shooting, in defense of civil liberties. Bowing to public pressure, the FBI voluntarily withdrew its request a few weeks later and Apple, in turn, requested that the court drop the case. Such a result is unlikely to occur in countries such as Russia or PRC, where national interest is paramount, telecommunication networks are publicly owned, and robust national surveillance programs are in place.

In Russia, the country’s data localization legislation is officially known as Federal Law No. 242-FZ. The final amendments to this data localization law went into effect on Sept. 1, 2015 and requires that all domestic and foreign companies accumulate, store and process personal information of Russian citizens on servers physically located within Russian borders.

In PRC, the country’s Cybersecurity law applies a very broad definition of “critical information infrastructure”. In an update to the law, the wording of this phrase was changed to “important data”, further broadening the law’s regulatory scope. While the law provides detailed explanations of data localization regulation, its broad terminology leaves room for unrestricted government intervention in any industry.

This lack of restriction raises the international business community’s concern of unwanted surveillance by the Chinese government. Additionally, discrepancies between the official version of the regulation and two updated drafts has lead to further confusion. With the official implementation of the data localization regulation being delayed until the end of 2019, speculation exists on how it will evolve. However, what is known for sure is that PRC’s data localization will remain all-embracing – fulfilling PRC’s dedication to building cyber sovereignty.
The international privacy landscape will continue its fast-changing pace through 2019.

UNITED STATES

In the United States, a phase of deregulation on the federal level will continue under the Trump administration, however individual states are enacting privacy-related bills independently. In the United States, there is no single, comprehensive federal law regulating the collection and use of personal data. However, with each Congressional term, proposals are introduced to standardize laws at the federal level. However, these are yet to become law and instead the United States has a patchwork system of federal and state laws and regulations that sometimes overlap, dovetail and contradict one another. Additionally, there are many guidelines, developed by governmental agencies and industry groups, that do not have the force of a law, but are part of self-regulatory guidelines and frameworks that are considered “best practices”. These self-regulatory frameworks have accountability and enforcement components that are increasingly being used as a tool for enforcement by regulators.20

In addition, various states, including Alabama, Arizona, California, Colorado, Iowa, Louisiana, Nebraska, Oregon and Virginia, have privacy bills pending or due to be effective. Perhaps the most high-profile one is California’s Consumer Privacy Act (CCPA, A.B. 375), which has a nickname of “mini GDPR”. Approved in June 2018, it’s likely to have some amendments by its effective date of January 2020.21 This new law gives consumers broad rights to access and control their personal information, and imposes technical, notice and financial obligations on affected businesses.

Enacted to protect the privacy of California consumers, CCPA’s similar characteristics to the EU’s GDPR include a new and very broad definition of what is included in protected personal information22. Affected businesses are for-profit entities doing business in California that meet certain revenue or data collection volume requirements. Businesses will need to modify operations, policies and procedures to comply with California residents’ rights to their personal information. Given the requirement for the California Attorney General to develop implementing regulations, and strong and open opposition by technology companies, the final CCPA compliance requirements will likely evolve considerably between now and January 2020.23

BRAZIL

Also inspired by GDPR, Brazil enacted its General Data Protection Law – Lei Geral de Proteção de Dados (LGPD) (Law 13,709/2018) – in August 2018. The law is expected to take effect in early 2020 after its 18th adaptation period.

The LGPD creates a new legal framework for the use of personal data in Brazil, both online and offline in both the private and public sectors. It’s important to note that the country already has more than 40 legal norms at the federal level that directly and indirectly address the protection of privacy and personal data in a sector-based system. However, the LGPD is replacing and/or supplementing this sectoral regulatory framework, which was sometimes conflictive and unclear, without legal certainty, and made the country less competitive in the context of an increasingly data driven society24.
Similar to the GDPR, the LGPD sets out general principles that underpin all processing of personal data, and then builds on those principles by identifying specific legal bases that can be relied on to support particular acts of data processing. The ten general principles applicable to all data processing are detailed in Article 6. One key principle is “purpose limitation” – where all processing must be “for legitimate, specific and explicit purposes of which the data subject is informed”. Further, the principle of “necessity” requires “limitation of the processing to the minimum necessary to achieve its purposes”. Other key principles include “free access and transparency” to the data subject, as well as “data quality”, including the “accuracy, clarity, relevance and updating” of the personal data. Finally, the “accountability” principle requires the demonstration of the adoption of effective measures to ensure the protection of personal data. Importantly, while the LGPD focuses mostly on data privacy, the principles also impose substantive data security requirements, whereas companies must adopt “technical and administrative measures to protect personal data from unauthorized access and accidental or illegal destruction, loss, alteration, communication or dissemination.”

THE UNITED KINGDOM

While the UK’s Brexit plans remain unclear, Information Commissioner Elizabeth Denham sets out how the Information Commissioner’s Office (ICO) is helping businesses, particularly small and medium enterprises (SME), prepare for a possible no-deal Brexit. The government has made it clear that the GDPR will be absorbed into UK law at the point of exit, so there will be no substantive change to the rules that most organizations need to follow. However, organizations that rely on the transfer of personal data between the UK and the European Economic Area (EEA) may still be affected.

OTHER NATIONS

It’s worth noting that other nations, including India, Thailand, Japan, Australia and South Africa, all have privacy legislation similar to, if not identical to, the GDPR that’s due to be effective in 2019.
As the EU’s GDPR legislation dominated headlines in 2018, the ePrivacy Regulation will be the next one to grab headlines in 2019. However, this regulation isn’t just about cookies. It concerns electronic communications and the right to confidentiality, data and privacy protection, and more. In other words, personal data protection – again.

Electronic communications include the Web, the Internet (email, apps, you name it), the telephone, instant messaging and so on. Also of relevance is spam and direct marketing, as well as telecommunication firms, mobile app developers, online advertising networks, and the often overlooked Internet of Things (IoT), among many others. This involves examining the text and impact of communications. As the EC made clear in its GDPR progress report of EU member states, all focus remains on the GDPR at this time. It’s most likely that the ePrivacy Regulation will NOT enter into force until probably the second half of 2019.27

WHAT DOES THIS MEAN TO US?

Besides the United States-China division, internet fragmentation is also occurring in less obvious places, according to Oxford cybersecurity expert Emily Taylor. Europe’s GDPR has led some companies to overreact and block their sites from European visitors. Moreover, other jurisdictions are following suit and considering data localization laws. Taylor warns, “You’re going to end up with cross-cutting national and regional laws that are reaching over their borders, making it very difficult for companies to comply. People will just choose to be very limited in what they do and the audiences that they try to reach.”28

After a year of scandals, the implementation of Europe’s GDPR and upcoming implementation of similar legislation from other jurisdictions, the advertising business will move away from the wholesale collection of personal data and the extreme personalization of advertising, predicts Mihael Mikek, the founder and CEO of digital advertising platform Celtra. “The question will come down to – is the data being used in a way that benefits the consumer or not?” he explains. “In the last five years, it’s been such a crazy race to collect as much as possible.” Advertisers will follow consumers, who will demand more ethical and consent-based use of their data. And, considering The New York Times’ investigation of location-tracking apps, location data is likely to be the next battlefront.29
LOOKING AHEAD

The global privacy landscape will continue to evolve as multinational and regional organizations push ahead with their quest for data. Bill Gates predicts the balance between privacy and innovation is an area to watch in 2019.

Key questions include: How can we use data to gain insights into education, such as which schools do the best job of teaching low-income students, or health, such as which doctors provide the best care for a reasonable price, while protecting people’s privacy?

The intensity of privacy demands from consumers will rise in tandem with broadening privacy legislation and corporate big data capacities. In 2019, this will likely result in some high-profile lawsuits based on this tension and the rebalancing of stakeholder relationships.
REFERENCES


7. https://www.linkedin.com/pulse/coming-big-tech-backlash-don-peppers/?trk=eml-email_feed_ecosystem_digest_01-recommended_articles-7-Unknown&midToken=AQHLKtPA-NGCNg&fromEmail=fromEmail&ut=1veVEoNNt1YUw1


20. https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1
27. https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/
30. https://www.linkedin.com/pulse/what-i-learned-work-year-bill-gates/?trk=eml-email_feed_ecosystem_digest_01-recommended_articles-11-Unknown&midToken=AQHLKtPA-NGCNg&fromEmail=fromEmail&ut=0tU0aQc7lAJEA1
ADDITIONAL REFERENCES


+ The International Association of Privacy Professionals (IAPP) - https://iapp.org/


+ South Korea - Personal Information Protection Act (Act No. 14839) (PIPA) https://content.next.westlaw.com/Document/I1d81ec834f271e498db8b09b4f043e0/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1


Dr. Jessica Santos is the Global Compliance and Quality Director at Kantar Health, a leading global healthcare consulting and market research firm focused in the life sciences industry. She is primarily responsible for providing oversight and support across Kantar Health’s global offices in the areas of regulation, interaction with clients, suppliers and others within Kantar Health, Kantar and WPP. Dr. Santos is responsible for maintaining, anticipating and coordinating all activities with regard to compliance laws/regulations, industry guidelines, pharmacovigilance and client contracts, defining and driving the execution of Kantar Health’s Quality Strategy – its approach to measuring and improving quality efforts.

Dr. Santos is an experienced statistician, analyst, methodologist and market research scientist. She gained her reputation through her publications and professional committee work in the industry. She is a frequent speaker and contributor in major conferences and has a Ph.D. in Marketing, an MRS fellowship and Chartered Marketer status.

Dr. Santos is a member of UK Research Ethics Committee, EphMRA, BHBIA and PMRG Government Affairs Committee, reviewer and co-chair of ISPOR, and MRS Professional Development Advisory Board and Examiner.