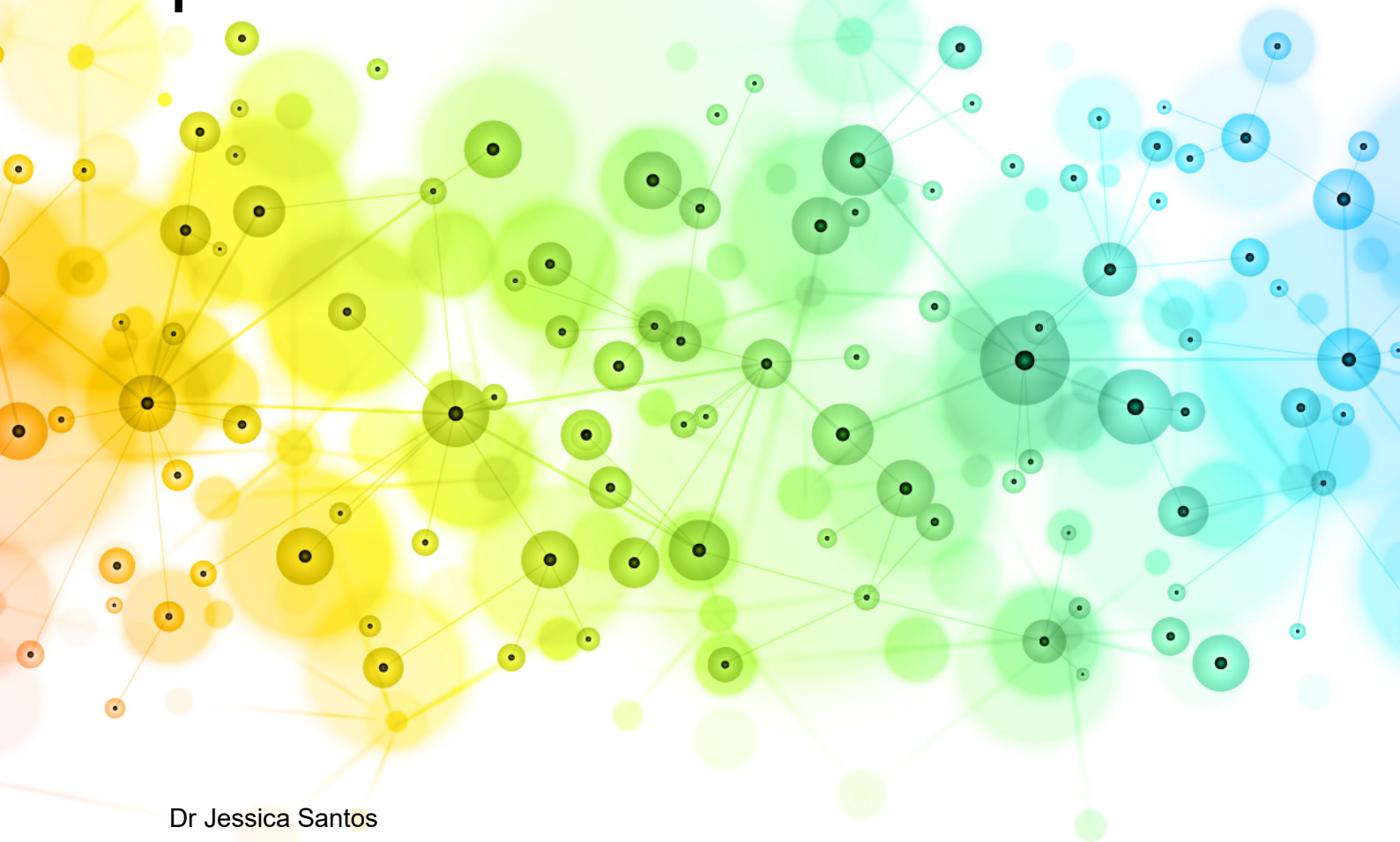
LiGHTSPEED

International landscape of privacy legislation, past, present and future



Dr Jessica Santos

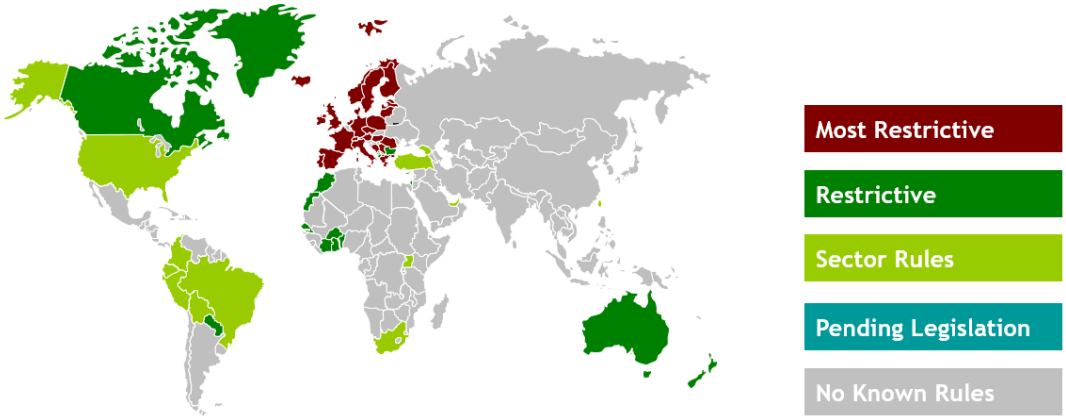
Dec. 2018 / Jan 2019

LiGHTSPEED

Global privacy landscape changed dramatically in the beginning of this millennium. On the one hand, data is regarded as power and the new commodity or even currency[1], on the other hand, both data subjects and regulators have increasing demand of data privacy to avoid personal data violation.

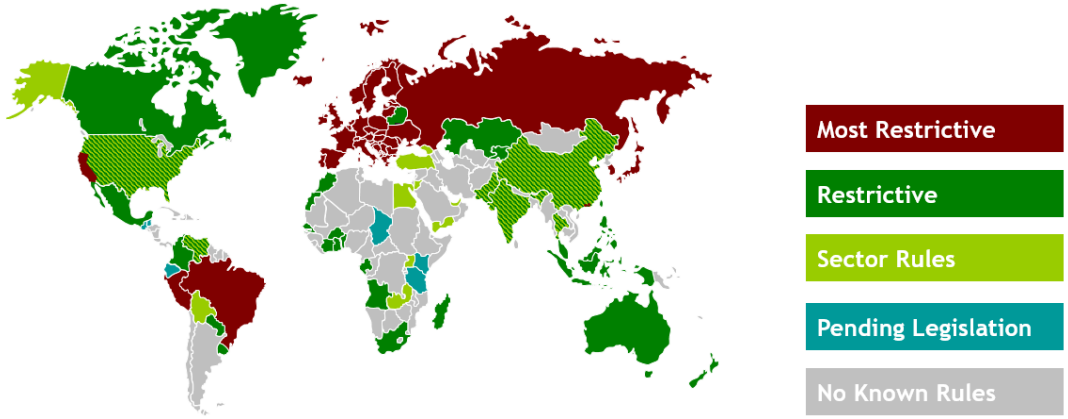
Global Privacy Landscape From 2001 to 2018

Privacy Regulatory Landscape in 2001



To 2018

Privacy Regulatory Landscape in 2018



[1] https://www.forbes.com/sites/michelleevans1/2018/03/12/why-data-is-the-most-important-currency-used-in-commerce-today/

LiGHTSPEED

Reference: Data Protection Laws of the World, DLA Piper - https://www.dlapiperdataprotection.com/index.html#handbook/world-map-section

Principles of Privacy – Human Rights? Commodity or State Interest

There is no universal consistency of the principle of the data protection or how personal data are regarded. The difference of Interpretation of privacy is largely based on the founding principle of each country/region, hence the legislations laid out thereafter, and more importantly enforcement actions.

There are three broad categories of privacy interpretation:

1. **Privacy is a human right**
   In the EU, human dignity is recognised as an absolute fundamental right. In this notion of dignity, privacy or the right to a private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role. Privacy is not only an individual right but also a social value. [2]

   Countries have adequate status from EC, such as Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Jersey, Japan, New Zealand, Guernsey, Israel, Isle of Man and Uruguay are sharing this principle.

   Almost every country in the world recognises privacy in some way, be it in their constitution or in other provisions. Moreover, privacy is recognised as a universal human right while data protection is not – at least not yet. The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12)[3], the European Convention of Human Rights[4] (Article 8) and the European Charter of Fundamental Rights[5] (Article 7).

   The most famous piece of legislation in 2018 – GDPR - is to enforce this principle and 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, and also sets minimum standards on use of data for policing and judicial purposes.

Europeans, after all, have consistently shown a significantly lower tolerance for privacy invasion than Americans have, perhaps related to their experience with various all-knowing, totalitarian regimes in the last century[6].

[2] https://edps.europa.eu/data-protection/data-protection_en
[3] http://www.un.org/en/universal-declaration-human-rights/
[4] https://www.echr.coe.int/Documents/Convention_ENG.pdf
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN
[6] 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

2. **Privacy can be a commodity**
   Historically, in other 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 distinction between Europe and other parts of the world is relative since it is also an element of privacy in the EU.

   The supreme law in the US is the US Constitution, drafted originally by the Constitutional Convention in 1787[7]. The US Constitution does not contain the word 'privacy'.[8] The right to privacy most often is protected by statutory law. For example, the Health Information Portability and Accountability Act (HIPAA)[9] protects a person's health information, or the Children's Online Privacy Protection Act (COPPA)[10], the Gramm-Leach-Bliley Act (GLBA[11]) and the Federal Trade Commission (FTC) enforces the right to privacy in various privacy policies and privacy statements.

   It is common to refer data as 'assets' in the US[12], which can be sold, purchased or transferred from one entity to another with a price tag, especially in the era of Big Data[13]. Data as a business asset is often listed in corporate balance sheet, MSA (Master Service Agreement) and in merge acquisition deals.

   The right to privacy often must be balanced against the state's compelling interests, including the promotion of public safety and improving the quality of life. Seat-belt laws and motorcycle helmet requirements are examples of such laws. And while many Americans are quite aware that the government collects personal information, most say that government surveillance is acceptable.[14]

3. **Privacy is secondary to state interest** (Russia, China)
   Most countries have the protection of 'national interest' in their constitution, yet its conflict with personal privacy is ongoing. A trade-off or compromise is not easily balanced.

   For example, Apple boss Tim Cook refused to cooperate with a US government to unlock an iPhone used by Syed Farook, one of the two shooters in the San Bernardino attack, was a defense of civil liberties[15]. A few weeks later, the FBI voluntarily withdrew its request to Apple and asked Judge Sheri Pym to drop the case[16]. Such case is unlikely to happen in countries such as Russia or China, where

---

[7] https://history.state.gov/milestones/1784-1800/convention-and-ratification
[8] Swire P. and Ahmad K. (2012) 'US Private Sector Privacy, Law and Practice for Information Privacy Professionals', IAPP
[9] https://www.hhs.gov/hipaa/index.html
[10] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
[11] https://www.fdic.gov/regulations/compliance/manual/8/viii-1.1.pdf
[12] https://www.i-scoop.eu/big-data-action-value-context/data-business-asset/
[13] https://www.information-age.com/data-listed-balance-sheet-business-asset-123469799/
[14] https://www.livescience.com/37398-right-to-privacy.html
[15] https://www.theguardian.com/technology/2016/feb/22/tim-cook-apple-refusal-unlock-iphone-fbi-civil-liberties
[16] http://www.lex-warrier.in/2017/11/privacy-national-interest/

national interest is paramount, and telecommunication communication network are dominantly public owned or funded with robust national surveillance program.

Russia's data localization legislation is officially known as Federal Law No. 242-FZ. The final amendments to this data localization law in Russia went into effect on September 1, 2015, and required all domestic and foreign companies to accumulate, store, and process personal information of Russian citizens on servers physically located within Russian borders[17]. The obligation is on all data operators to ensure the recording, systematisation, accumulation, storage, change and extraction of personal data of Russian citizens with the use of data centres located in the territory of the Russian Federation. [18]

People's Republic of China (PRC)'s Cybersecurity law uses a very broad definition of "critical information infrastructure." In later wording this phrase was changed to "important data," further broadening the regulating scope. The law provides detailed explanations of data localization regulation, but broad terminology leaves room for unrestricted government intervention in any industry. The lack of restriction adds to, instead of appeasing, the international business community's concern of being surveilled by the Chinese government. In the meantime, the discrepancies between the official versions of the regulation and the two updated drafts leads to confusion. As the official implementation of data localization regulation has been delayed until the end of 2019, how it will evolve is still the realm of speculation; but what is known for sure is, China's data localization will remain to be all-embracing, fulfilling China's dedication to building cyber sovereignty.[19]

[17] https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy/
[18] https://uk.practicallaw.thomsonreuters.com/2-502-2227?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1
[19] https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/

LiGHTSPEED

Forthcoming Privacy Landscape

The fast-changing privacy landscape will continue gather its pace in 2019.

The **US** is going through a phase of deregulation on the federal level under Trump administration, but different states are enacting privacy related bills independently. In the US, there is no single, comprehensive federal (national) law regulating the collection and use of personal data. However, each Congressional term brings proposals to standardise laws at a federal level. Instead, the US has a patchwork system of federal and state laws and regulations that can sometimes overlap, dovetail and contradict one another. In addition, there are many guidelines, developed by governmental agencies and industry groups that do not have the force of 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]

States including **Alabama, California, Colorado, Arizona, Iowa, Louisiana, Nebraska, Carolina, Oregon, Virginia, Dakota** all have privacy bills pending or due to be effective. The most famous one is **California Consumer Privacy Act (CCPA,** A.B. 375**)**, which has a nickname of 'mini GDPR'. It is unanimously rammed on June 28 2018, likely to have some amendments by effective data - Jan 1 2020.[21] The new law gives consumers broad rights to access and control of their personal information and imposes technical, notice, and financial obligations on affected businesses, see below.

- "Annual gross revenues in excess of" $25 million;
- "Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices";
- "Derives 50 percent or more of its annual revenues from selling consumers' personal information."

CCPA was enacted to protect the privacy of California consumers and has some similar characteristics to the EU's General Data Protection Regulation (GDPR), including a new and very broad definition of what is included in protected personal information[22]. 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 information about and control of their personal information. Given the requirement for the California Attorney General to develop implementing regulations, and the strong and open opposition to the CCPA by technology companies, the final compliance requirements will likely evolve considerably between now and January 1, 2020[23].

Also inspired by GDPR, **Brazil** enacted its General Data Protection Law – Lei Geral de Proteção de Dados (**LGPD**) (Law 13,709/2018) in Aug 2018. The law will come into effect after its 18th adaptation period, in early 2020.

---

[20] https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&comp=pluk&bhcp=1

[21] https://www.caprivacy.org/

[22] https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/

[23] https://privacylaw.proskauer.com/2018/09/articles/california/california-legislature-passes-amendments-to-the-california-consumer-privacy-act/

The LGPD creates a new legal framework for the use of personal data in Brazil, both online and offline, in the private and public sectors. It is important to note that the country already has more than 40 legal norms at the federal level that directly and indirectly deal with 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, marshy, without legal certainty and made the country less competitive in the context of an increasingly data driven society[24].

Similar to the GDPR, the LGPD sets out general principles that must 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 spelled out in Article 6. A key principle is purpose limitation—i.e., all processing must be "for legitimate, specific and explicit purposes of which the data subject is informed." The principle of necessity likewise 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,
and data quality—i.e., the "accuracy, clarity, relevance and updating" of the personal data. The "accountability" principle requires demonstrating the adoption of effective measures to ensure protection of personal data. Importantly, while the LGPD focuses mostly on data privacy, the principles also impose substantive data security requirements: companies must adopt "technical and administrative measures to protect personal data from unauthorized access and accidental or illegal destruction, loss, alteration, communication or dissemination."[25]

In addition, **India, Thailand, Japan, Australia and South Africa** all have privacy legislation similar if not identical to GDPR due to be effective in the coming months.

As **EU's GDPR** legislation dominated headline in 2018, the ePrivacy Regulation will be the next one to pay attention. It isn't just about cookies. It concerns electronic communications and the right of confidentiality, data/privacy protection and more. In other words: again, personal data protection.

Electronic communications means that it includes the Web, the Internet (email, apps, you name it), telephone, instant messaging and so on. So we are also talking about spam, direct marketing, telecommunication firms, mobile app developers, online advertising networks and, often overlooked, the IoT (Internet of Things), among many others. A look at the text, the impact, the challenges and the evolutions. As the European Commission made clear in the scope of the progress of EU member states with the GDPR, all focus is on the GDPR at this time and it is pretty sure that the ePrivacy Regulation will NOT enter into force before 2019 and even most probably the second half of 2019.[26]

UK's Brexit and future relationship with EU might not be certain, Information Commissioner Elizabeth Denham sets out how the ICO is helping businesses, particularly SMEs, prepare for a possible no-deal Brexit. The Government has made clear that the General Data Protection Regulation (GDPR) will be absorbed into UK law at the point of exit, so there will be no substantive change to the rules that most organisations need to follow. But

[24] https://iapp.org/news/a/the-new-brazilian-general-data-protection-law-a-detailed-analysis/

[25] https://www.debevoise.com/~/media/files/insights/publications/2018/08/08202018_the_brazilian_data_protection_law_lgpd.pdf

[26] https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/

organisations that rely on the transfers of personal data between the UK and the European Economic Area (EEA) may be affected.[27]

What does this mean to us?

Besides the U.S.-China division, internet fragmentation is also happening in less obvious places, Oxford cybersecurity expert Emily Taylor explains. Europe's global data protection regulation (GDPR) has led some companies to overreact and block their sites to European visitors. Other jurisdictions are following suit and considering data localization laws. "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," Taylor warns. "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 copycat 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. After The New York Times' investigation of location-tracking apps published yesterday, location data is likely to be the next battlefront.[29]

The intensity of privacy demand from consumers, ever increasing privacy legislations and big data capacities of corporation are increasing. 2019 is likely to see some high-profile lawsuits of based on this tension and rebalance this relationship.

[27] https://ico.org.uk/about-the-ico/news-and-events/blog-data-protection-and-brexit-ico-advice-for-organisations/
[28] https://www.linkedin.com/pulse/50-big-ideas-2019-what-watch-year-ahead-isabelle-roughol/
[29] https://www.linkedin.com/pulse/trends-workplace-what-you-need-know-bigideas2019-kim-peterson-stone/?trk=related_artice_Trends%20in%20the%20workplace.%20What%20you%20need%20to%20know%20%23BigIdeas2019%20%0A%0A_article-card_title

LIGHTSPEED

Additional Reference:

1. General Data Protection Regulation (GDPR) - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1462359521758&from=EN
2. The International Association of Privacy Professionals (IAPP) - https://iapp.org/
3. India – Personal Data Protection Bill - http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdfDifferent
4. Japan - The Act on the Protection of Personal Information ("APPI") http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf
5. Australia Privacy Act - https://ballawyers.com.au/2018/01/28/privacy-act-changing/
6. South Korea - Personal Information Protection Act (Act No. 14839) (PIPA) https://content.next.westlaw.com/Document/I1d81ec834f2711e498db8b09b4f043e0/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1
7. South Africa- The Protection of Personal Information Act (POPI) http://www.saica.co.za/Technical/LegalandGovernance/Legislation/ProtectionofPersonalInformationAct/tabid/3335/language/en-ZA/Default.aspx
8. Thailand - Thailand Draft Personal Data Protection Act - https://www.dataprotectionreport.com/2018/08/overview-of-thailand-draft-personal-data-protection-act/