P.O. Box 5675, Berkeley, CA 94705 USA

Data Privacy - How a Lack of Uniformity is Detrimental to Progress

Contact Information:
Amal Assioua, Frank C. Newman Intern
Representing Human Rights Advocates through
University of San Francisco School of Law's
International Human Rights Clinic
Tel: 415-422-6752
assioua@usfca.edu
Professor Connie de la Vega
delavega@usfca.edu

I. Introduction

The right to privacy is not only a fundamental freedom under international law, it is also a right declared in over 150 national constitutions.[1] Human rights and fundamental freedoms that people enjoy offline, which are enshrined in the Universal Declaration of Human Rights ("UDHR"), and relevant international human rights treaties, including the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR"), must equally be guaranteed and protected. [2]

Today, we live in a technologically driven society which stretches beyond the confines of legal standards that were set more than thirty years ago. Social media for example has blurred the line between what's private and what's public through practices such as data monetization and target advertising. The Right to Privacy extends beyond the person or the home. "Recognizing that the right to privacy can enable the enjoyment of other rights and the free development of an individual's personality and identity, and an individual's ability to participate in political, economic, social and cultural life, and noting with concern that violations or abuses of the right to privacy might affect the enjoyment of other human rights, including the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association."[3]

The exercise of human rights in the Digital Age, in particular the right to privacy, is an issue of increasing interest and importance as the rapid pace of technological development allows persons all over the world to use digital technologies. In an ideal world, data protection would be harmonized across continents to ensure a more comprehensive and coherent global

[1] World constitutions, constituteproject.org, 31 March 2018.
[2] Report of Special Rapporteur on the Right to Privacy, A/HRC/ 37/ 62, 28 February 2018.
[3] Human Rights Council Resolution, the Right to Privacy in the Digital Age, A/HRC/RES/34/7, 23 March 2017.

policy on the fundamental right to personal data protection, especially in the extraterritorial application of data. There is no question that the global community needs to undertake urgent action to effectively respect and implement article 12 of the UDHR and article 17 of the ICCPR by developing a comprehensive legal framework on privacy in cyberspace, and to operationalize the respect of this right, domestically and across borders.[4] Unless and until it will be possible for any citizen, anywhere, irrespective of their passport, to enjoy privacy protection without borders and privacy remedies across borders, then it cannot be said that a clear and comprehensive legal framework exists.[5] In order to create such a clear and comprehensive legal framework, it is essential that an international legal regime regulating issues of jurisdiction in cyberspace be properly developed with a commonly agreed set of principles.[6]

II. Background

A. Data Protection Versus Data Privacy Distinction

Data privacy and data protection are very closely interconnected, so much so that users often think of them as synonymous. But the distinctions between data privacy and data protection are fundamental to understanding how one complements the other. Privacy concerns arise wherever personally identifiable information is collected, stored, or used.

> In a nutshell, data protection is about securing data against unauthorized access. Data privacy is about authorized access—who has it and who defines it. Another way to look at it is this: data protection is essentially a technical issue, whereas data privacy is a legal one. These distinctions matter because they're woven deeply into the overarching issues of privacy and cybersecurity, both of which loom large in businesses, politics and culture. For industries subject to compliance standards, there are crucial legal implications associated with privacy laws. And ensuring data protection may not adhere to every required compliance standard.[7]

[4] *Id.*
[5] *Id*.
[6] *Id.*
[7] Data Privacy vs. Data Protection, Rick Robinson, https://blog.ipswitch.com/data-privacy-vs-data-protection, 29,01,2018.

A. The Right to Privacy as It Stands Today

1. International Standards

While international human rights law provides universal rules for the protection of the right to privacy, it lacks the level of detail necessary to provide adequate protection.[8] Most regions in the world lack enforcement mechanisms such as those created over the past 40 years in Europe and North America.[9] Thus, the international legal framework would benefit from vastly increased detail, clarity and comprehensiveness, as well as safeguards and remedies for the daily violations of the right to privacy occurring in cyberspace.[10]

During its thirty-seventh session, the Human Rights Council (HRC) adopted a resolution recalling all previous resolutions adopted by the General Assembly (GA) and the HRC on the right to privacy in the digital age.[11] As a result, the HRC extended the mandate of the Special Rapporteur on the right to privacy for a period of three years under the same terms as provided for by the HRC in its resolution 28/16 of 26 March 2015.[12]

Pursuant to the HRC resolution 28/16, the Special Rapporteur focused its work on surveillance and privacy as they relate to the following thematic action streams: 1) developing a deeper understanding of privacy laws, 2) studying security and surveillance issues, 3) defining Big Data and Open Data, 4) researching Health Data, and 5) understanding how businesses use personal data.[13]

---

[8] *Id.*
[9] Report of Special Rapporteur on the Right to Privacy, A/HRC/ 37/ 62 (28 February 2018).
[10] *Id.*
[11] Privacy In The Digital Age, A/HRC/RES/28/16 (26 March 2015).
[12] HRC, Privacy In The Digital Age, A/HRC/RES/28/16, 26 March 2015.
[13] Right to Privacy in the Digital Age, A/HRC/RES/37/2 (22 March 2018).

The Special Rapporteur has put forth draft text on Government-led Surveillance and Privacy—which will ultimately aid states and the multi-stakeholder community to protect, respect and promote human dignity[14]—as the result of meetings and exchanges between leading global technology companies, experts with experience in working within civil society, law enforcement, intelligence services, academics and other members of the multi-stakeholder community shaping digital technology and the transition to the Digital Age.[15]

Human Rights Advocates (HRA) focuses this report and recommendations on the most robust laws currently governing use of personal data by businesses, specifically as they relate to the European Union's ("EU") supervisory authority General Data Protection Regulation ("GDPR")[16], deemed as the "model" framework upon which other countries look to for guidance; the amended Japan Act on Protection of Personal Information ("APPI"),[17] and the California Consumer Privacy Act of 2018 ("CaCPA"),[18] which will take effect in 2020.

III. Application Under Present Standards

Today, international standards and country standard for data privacy and data protection are viewed as distinctly different.

A. The Current Regulatory Framework

1. General Overview

Globally, there is an increasing growth in data and privacy protection laws, many of which have been modelled on robust data privacy frameworks such as that of the EU, but these are not widespread. According to the United Nations Conference on Trade and Development

[14] Report of Special Rapporteur on the Right to Privacy, A/HRC/ 37/ 62, 28 February 2018
[15] *Id.*
[16] GDPR, Art. 4(1)
[17] APPI, Art. 2(1), (3), (6)-(7)
[18] The Consumer Right to Privacy Act of 2018 -Version 2 No. 17-0039, October 12, 2017

("UNCTAD") data protection tracker,[19] over 107 countries around the world now have data protection laws in place. Based on this tracker, 58% of countries have passed legislation, 10% of countries have draft legislation, 21% of countries have no legislation, and 12% of countries have no data available.[20] The sheer increase in data protection laws across the world is testament to data protection's rising importance on the global agenda, however, not all laws are created equal.[21] There is a varying level of flexibility with which countries implement data protection requirements, which leads to confusion and inefficiency for any business navigating the current laws.

To put this in perspective, in order for a company to conduct business on the world wide web, it must comply with domestic as well as the following international laws: 1) GDPR if the business avails itself to EU customers;[22] 2) laws of each of the 19 African countries which have enacted data protection and privacy laws;[23] 3) the African Union laws on the progressive Convention on Cyber Security and Personal Data protection;[24] 4) the Economic Community of West African States (ECOWAS) Supplementary Act A/SA.1/01/10 on Personal Data Protection;[25] 5) several Francophone countries which promote personal data protection principles and rules in French-speaking countries; 6) legislation in the Asia Pacific, which include Australia and New Zealand;[26] 7) 15 countries in Asia; 8) the Asia-Pacific Economic Cooperation

[19] Data Protection and Privacy Legislation Worldwide, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx,UNCTAD, 01/04/2018
[20] *Id.*
[21] Consumers International, The State of Data Protection Rules Around the World, https://www.consumersinternational.org/media/155133/gdpr-briefing.pdf, (last visited Feb. 22, 2019)
[22] UNCTAD, 01/04/2018
[23] Id.
[24] Id.
[25] Id.
[26] Id.

(APEC);[27] 9) and legislation of 17 countries in The Americas and the Caribbean Across North America and Latin America.

To remedy this problem, the EU has recognized as compliant other frameworks outside its own which have been modeled after the GDPR, such as EU-US Privacy Shield Framework. This Framework was designed by the United States ("U.S.") Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the U.S. in support of transatlantic commerce. This practice is also known as "whitelisting." Latin American countries are also part of the Ibero-American Data Protection Network (RIPD),[28] which consists of 22 Data Protection Authorities. However, the only other non-EU countries that have data protection laws considered adequate by the EU are Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the U.S. Australia, New Zealand, Hong Kong, and Japan have modelled their data protection laws off the OECD Guidelines. So, while the GDPR may be held up as a new gold standard, it could be ambitious to assume that others will reach it any time soon, considering that many countries across the globe have yet to put data protection laws in place or finalize existing draft legislation.

2. Robust Frameworks (GDPR, CACPA, APPI)

The EU, Japan, and California—three of the five world's largest economies—have developed some of the most sophisticated and robust frameworks on the planet. However, even these frameworks are largely inconsistent.

[27] Id.
[28] Id.

The GDPR, as the most rigorous framework, zealously regulates entities' processing of Personal Information ("PI") if such entity: (1) is established in the EU; (2) offers goods or services, irrespective of whether a payment of the individual is required, to individuals in the EU; and (3) monitors behavior of individuals in the EU.[29]

The European Union's GDPR requires businesses to protect the "personal data and privacy" of EU citizens for transactions that occur within the EU. However, the GDPR's data protection law has a much different view of personal identification information than the U.S. "GDPR compliance requires that companies use the same level of data protection for cookies as they do for stored personally identifiable information, such as social security numbers."[30] Cookies are a small number of data saved by an individual's personal web browser for the purpose of remembering information about the individual.

Originally enacted 10 years ago, APPI's most recent amendments came into effect on May 30, 2017.[31] While it does not provide the details of personal information protection, it establishes basic rules, and as such, APPI is a more moderate approach, especially because it applies to any business or organization supplying goods or services to a person in Japan and collecting PI.[32]

As of January 1, 2020, companies around the world will have to comply with additional regulations related to processing of personal data of California residents. Pursuant to the CACPA, companies must observe restrictions on data monetization business models, accommodate rights to access, deletion, and porting of personal data, update their privacy

[29] Supra
[30] Data Privacy vs. Data Protection, Rick Robinson, https://blog.ipswitch.com/data-privacy-vs-data-protection, 29,01,2018.
[31]Supra
[32] Supra

policies and brace for additional penalties and liquidated damages. CaCPA is the narrowest geographic framework as it applies only to organizations doing business in California.[33]

Apart from the concern of extraterritorial reach of GDPR, which many privacy experts view as a potential violation of sovereign rights of nations,[34] the current regulatory structure lacks clear guidance and understanding of fundamental issues upon which the regulation is built. It seems somewhat counterintuitive that regulators are zealously enacting Personal Data Privacy laws but fail to confidently define "personal information"— a core principle.

A. Impediments, Policy & Practical Implications

1. Problems with the Current Structure as It Relates to Businesses

In the age of social media and decentralized networks, technology companies are ubiquitous and their reach is virtually unstoppable. Some of the biggest regulatory challenges to date involve data breaches and data exploitation. Protecting the privacy of individual technology participants is difficult under the current less unified regulatory landscape. Furthermore, as our research shows, the impediment has less to do with the rigor of a singular framework and more to do with the lack of a uniform global definition laying out the standard.

To comply with GDPR alone, the world's 500 biggest corporations were on track to spend a total of $7.8 billion.[35] Businesses must appoint someone in the EU as a liaison with regulators, and many larger companies are required to designate a "data protection officer" responsible for compliance.[36] Microsoft Corp. has 300 engineers working to ensure its software is GDPR-compliant. At Krones AG, a 15,000-employee German producer of bottling equipment,

---

[33] Supra

[34] Daniel Lyons,GDPR: Europe's Tariffs by Other Means, http://www.aei.org/publication/gdpr-privacy-as-europes-tariff-by-other-means/,03 July, 2018.

[35] Consultants Ernst & Young.

[36] Bloomberg Businessweek, It'll Cost Billions for Companies to Comply With Europe's New Data Law, Jeremy Kahn, Stephanie Bodoni, Stefan Nicola, https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law, (21 March, 2018).

almost 60 people are involved in GDPR preparations.[37] "The bigger an organization is, the bigger a nightmare it is,"[38] says Julian Saunders, chief executive officer of Port, a U.K. startup selling software that helps clients control who gets access to data and creates audit trails to monitor privacy.

Absent a unified framework, smaller companies lack the resources to adopt every standard required by every jurisdiction. It is often the case that companies resort to cherry picking lax or unregulated jurisdictions while circumventing the more rigorous ones through geo-fencing, a method for virtually excluding specific geographic locations from access to a company's goods or services.[39] This is problematic because the varying standards not only deprive customers of a healthy marketplace, it also stifles growth in smaller companies that lack the resources to comply in all jurisdictions.

Although having bilateral recognition agreements between counties, such as the EU-US Privacy Shield Framework, is a tremendous step in the right direction, these agreements are still flawed due to the definitional differences that exist.

2. Definitional Gaps - Personal Information

GDPR broadly defines PI as "any information relating to an identified or identifiable natural person."[40] 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[37] Id.
[38] Id.
[39] International Association of Privacy Professionals,Geofencing, https://iapp.org/resources/article/geofencing/
[40] GDPR, Art. 4(1)

This definition is broad and fairly all-encompassing. It includes a) any information relating to an identified individual (i.e. which makes such info personal to that individual), or b) any information relating to someone who could be identified based on a variety of identifiers.[41]

APPI is slightly less ambiguous than GDPR as it defines PI as "any data that is in and of itself personal in nature (e.g., name, date of birth, etc.) and includes unique identifiers assigned to an individual."[42]

CaCPA defines PI as "any information that identifies or could identify an individual."[43]Though not exhaustive, CaCPA enumerates some examples of PI, such as purchase history, biometric data, geo-location data.

APPI definition of PI appears to be broader than CaCPA and GDPR by recognizing that there may be types of information that are not actual PI without an identifier.[44] For example, certain types of behavioral information (e.g., cookies, etc.) could be considered non-PI under the APPI if the identifiers are removed, while the CaCPA and GDPR may require a further analysis of whether the behavioral information identifies an individual.[45]

IV. Conclusion

Data protection and privacy regulations are now a priority for most countries across the world. This is a tremendous step in the right direction not only because of the sheer increase in regulatory frameworks, but also because this is a cause that most, if not all, countries agree on. Therefore, implementing efficient practices, whether it is adding categories of PI and updating the definition of unique identifiers to address changes in technology and privacy concerns, or

[41]GDPR EU, Personal Data, https://www.gdpreu.org/the-regulation/key-concepts/personal-data/, (last visited Feb.23,2019)
[42] APPI, Art. 2(1), (3), (6)-(7)
[43] CaCPA 1789.140(o)
[44] Michihiro Nishi, APPI to Align WIth GDPR, 24, September, 2018.
[45] APPI, Art. 2.

merging frameworks through whitelisting, will ensure that consumers are truly protected and businesses are thriving.

V. Recommendations

Recently, AT&T, Google, Amazon, Twitter and Apple testified in U.S. Senate hearings in favor of a unified privacy and data security law covering consumer personal data.[46] Effectively, each framework modeled a simplified version of GDPR—but there was agreement on some ideas: Calling for a standard definition of PI, letting consumers access and correct their personal data (deleting information as needed) and setting basic data security standards.[47]

While HRA agrees in part with the regulatory changes discussed in the Senate hearing, we also urge the Special Rapporteur to consider the following recommendations for the use of personal data by businesses:

1. To adopt a single overarching definition for PI, which shall include an exhaustive list of qualifiers and exclusions;
2. To adopt, or use as template, the most rigorous standard (such as GDPR) that overlaps with other frameworks and to which companies are already compliant;
3. To encourage "whitelisting" where jurisdictions with similar standards recognize each other's frameworks as valid;
4. To add carve-out provisions allowing businesses, which are already compliant, to be excluded.

[46] Yeki Faitelson, Data Privacy Disruption In The U.S., Forbes.com (link),12 December 2018.
[47] *Id.*