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

GROWING NEED FOR A GLOBAL MINIMUM STANDARD OF CARE FOR PERSONAL DATA PROTECTION AND FOR SPECIAL PROTECTIONS FOR VULNERABLE POPULATIONS

Contact Information:
Carolina Quesada Ponce, 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
ciquesadaponce@usfca.edu
Professor Connie de la Vega
delavega@usfca.edu

What is understood as part of the right to privacy today, is vastly different from when the right was first recognised on the Universal Declaration of Human Rights adopted by the United Nations General Assembly on 1948. Before the growth of the digital era the right concerned mostly the person, their own dwelling, and correspondence. However, today's privacy rights encompass also the personal information that can be accessed and stored online, and any photographs or videos taken of a person.

In essence privacy rights concerns the protection of personal autonomy, prohibition of unlawful and arbitrary interference, and unlawful attacks to a person's reputation. Yet when talking about privacy rights in the digital area it is not enough to talk about the right to privacy, but it is also necessary to talk about corporate responsibility because it is mostly through Non-State actors, like companies, who are carrying out the .privacy rights violations.[1] As pointed out in the Special Rapporteur 2019 Report on Privacy Rights, it is important to protect individuals' personal information online as it concerns a person's autonomy and personal decision making.[2] Certainly, significant strides have been achieved in protecting individuals' information from being sold, shared, improperly used, or accessed without their consent or knowledge, but not enough to effectively protect privacy rights.

Countries have yet to reach an agreement on the minimum standard of care needed when dealing with people's information. Without a consensus on the protections that

[1] Yilma, Kinfe Michael, "The United Nation's Evolving Privacy Discourse and Corporate Human Rights Obligations," American Society of International Law, Vol. 23, Issue 4, (May 17, 2019), available at: https://www.asil.org/insights/volume/23/issue/4/united-nations-evolving-privacy-discourse-and-corporate-human-rights

[2] Special Rapporteur on the Right to Privacy, The Right to Privacy in the Digital Age, ¶ 7, U.N. Doc. A/HRC/RES/42/15 (October 7, 2019)

should be in place or what type of information should be protected, personal information is at jeopardy of being distributed or accessed without owner's consent since Non-State and State actors are improperly sharing, storing, and profiting from collected individuals' information. There is a need for States to adopt a universal standard for the protection of people's digital private personal information.

One of the major problems with ensuring an adequate level of data protection is due to the very nature of digital information — it can be accessed from anywhere. Therefore, even where regions have comprehensive data protection regulations, States have little power over Non-State actors that operate outside of the jurisdiction. For instance, in the European Union ("EU"), which has legislated to ensure substantial protections for their citizens, individuals' data is still at risk. Even when the legislation requires outside non-state actors to comply with the regulation there is a question as to the extraterritoriality, hence its enforceability and reach. It is crucial that all States adopt measures with the same standard of care and diligence ensuring people's personal data is protected.

However, not only is there a need for a global minimum standard of care for data protection, but for additional protections to be placed for vulnerable populations such as women, lesbian, gay, bisexual, transgender, and queer people ("LGBTQ"), and immigrants. It is important to create these protections to protect the above-named groups from discrimination, unwanted and unwarranted exposure, improper surveillance, harassment, and address power imbalances in the exercise of privacy rights. Especially

when addressing women and people in the LGBTQ community, there is a concern that gender-based violence is exacerbated by the lack of protection on privacy rights.

I. Digital Privacy Rights

The right to privacy is a fundamental right that has long been recognised by governments around the world. The first time the international community recognised the right to privacy was in the Universal Declaration of Human Rights Article 12 where it is provided that:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Yet, the right is not seen as an absolute right, meaning that certain limitations have been placed in order to ensure the State can protect everyone's privacy right.

Digital privacy rights concern not only the accumulation of personal data stored online, but also how the information stored is protected from attacks (cybersecurity). Currently the most concerted effort in addressing and evaluating cybersecurity is by the United Nations through its International Telecommunication Union, which conducts the Global Cybersecurity Index. The index's purpose is to determine the status of cybersecurity worldwide and promote global harmonization of cybersecurity legislation.

II. Current Legislation on Digital Privacy Rights

Discussions and regulations on the right to privacy need to be addressed at a domestic and international level to be effective otherwise the gaps in protection still leave data at

risk. Lack of such protections could lead to undue influence on individuals' human rights.[3] Following are examples of legislation on data protection, cyber security, and surveillance and the effects.

a) EU General Data Protection Regulation

The General Data Protection Regulation ("GDPR") is perceived as a groundbreaking legislation that addresses many of the concerns of data protection. The legislation addresses not only data protection but also cyber security; it has also provided a standard of care and regulation for all the EU and guidelines on how to enforce the legislation. In article 4 of the GDPR, delineates one of the most comprehensive definitions of personal data:

> '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."[4]

GDPR's Article 4 is one of the most comprehensive definitions not only because it mentions in detail what type of personal data it regulates, but also because it qualifies as personal data any combination of the stored data leading to "directly or indirectly"[5] identifying the subject of the data. GDPR is consumer-first focused, therefore it is aimed at protecting individuals' information. Allowing for a combination of stored data to suffice

---

[3] Human Rights Council Res. 42/15, The Right to Privacy in the Digital Age. U.N. Doc. A/HRC/RES/42/15 (Sep. 26, 2019)
[4] European Union, General Data Protection Regulation, Art. 4, available at: https://gdpr.eu/eu-gdpr-personal-data/
[5] *Id.*

the definition of personal data, permits for a more extensive protection of personal data. Complying with GDPR's regulation on data protection means ensuring data is collected legally, informing users of how it is treated, and keeping data secure. The legislation establishes that controller and processor of personal data must put in place "appropriate technical and organizational measures to implement the data protection principles."[6] Despite how compressive the regulation is, several issues have risen.

The GDPR applies to entities that although operate outside Europe or the European Economic area, must adhere to GDPR guidelines and requirements if they transact with people in Europe. The reach of the GDPR has prompted concerns over the extraterritoriality reach of the legislation because it is asking Non-State actors and States outside of the European Union, to adhere to GDPR which is a law most States around the world are not part of.

Critics of the GDPR state that the legislation has been successful as a "breach notification law," but has not been effective if protecting and preventing mishandling of information because EU officials are not properly imposing fines on those not adhering to the regulation. [7] The majority of the companies have still not been fined for failure to protect personal data and even if the companies are fined the fines are to small to make a real difference.[8] For the GDPR to achieve the goal for which it was created, it is necessary that authorities diligently monitor companies and enforce regulations when companies have failed.

---

[6] European Union, General Data Protection Regulation, Art. 25.2, available at: https://gdpr-info.eu/art-25-gdpr/
[7] Wolff, Josephine, "How Is the GDPR Doing?," Slate, (March 20, 2019), available at: https://slate.com/technology/2019/03/gdpr-one-year-anniversary-breach-notification-fines.html
[8] *Id.*

b) Paris Call for Trust and Security in Cyberspace

On November 12, 2018, French President Macron called for a worldwide effort from States and non-state actors to unite in an effort to combat, prevent and recover from malicious cyber activity that harm individuals and critical infrastructure, the call is commonly known as the Paris Call.[9] This type of legislation although greatly needed because it deals with cyber security and some digital privacy rights, the call does not address the problem that there is a need worldwide for legislation relating to surveillance, the need for comprehensive online personal data protections, and how State and non-State actors are allowed to access, store, or share the obtained information.

The Paris Call rests on 9 principles:

1) "Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.
2) Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet.
3) Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.

[9] "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace," French Ministry for Foreign Relations, available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

4) Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector.
5) Develop ways to prevent the proliferation of malicious software and practices intended to cause harm.
6) Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain.
7) Support efforts to strengthen an advanced cyber hygiene for all actors.
8) Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.
9) Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace."[10]

Many Non-state actors, specifically business, consider that technologies are essential to operation and therefore see that cybersecurity is a business strategy.[11] As internet dependency has increased, 68% of business leaders stated that cybersecurity risks have also increased.[12] The Paris Call has the potential for greater State and Non-State actor coordination and for achieving sustainable initiatives.

[10] "The 9 Principles," Paris Call" (November 12, 2018), available at: https://pariscall.international/en/principles
[11] Zwinggi, A, Pineda, M, Dobrygowski, D, and Lewis, R, "Why 2020 is a Turning Point for Cybersecurity," World Economic Forum, (January 23, 2020), available at: https://www.weforum.org/agenda/2020/01/what-are-the-cybersecurity-trends-for-2020/
[12] "The Cost of Cybercrime," Accenture Security, (2020), available at: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

c) California Consumer Privacy Act

The state of California in United States enacted a law in 2018, which entered into force on January 1, 2020 where it allows consumers to ask business to disclose the personal information the business has gathered on the individual, how it has shared such information, and gives the consumer the opportunity to opt-out from the business disclosing their information to third parties.[13] However, California[14] is the only state that has enacted this protection for their citizens so if the individuals' information is accessed in a different state, it in effect nullifies the state of California's efforts to protect its own citizens' private information. Hence, there is need a comprehensive federal privacy law in the United States[15] that would give users the right to have their personal data minimized, give users the right to know what data is collected on them, give users the right to access that data, and require that data be kept securely.

The United States lacks a national privacy law, instead each state has the power to regulate what or if privacy rights should be protected. However, there are a few very limited in scope federal laws that protects a specific type of data.

[13] CA Civ. Code Section 1798.100, available at: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375&search_keywords=California+Consumer+Privacy+Act+of+2018

[14] A criticism of California Privacy Law is that it lacks a gender perspective and does not address when privacy issues like revenge porn or the sharing of intimate photos. Chang, Emily, "What Women Know About the Internet," The New York Times, (April 10, 2019), available at: https://www.nytimes.com/2019/04/10/opinion/privacy-feminism.html

[15] United States in the Comparitech Assessment scored a 2.7 tying with Singapore because although there are some safeguards, there are weakened protections. The assessment also found that the countries with the best privacy protection are in the EU and accredits in part the GDPR to their data protection efforts. Bischoff, Paul, "Surveillance States: Which countries best protect privacy of their citizens?" Comparitech, (October 15, 2019), available at: https://www.comparitech.com/blog/vpn-privacy/surveillance-states/.

i. Need for Nation-Wide Privacy Laws in the United States

The United States lacks a comprehensive federal law that regulates the collection, storage, and usage of personal information. Instead, there is a patchwork of different regulations of specific sectors and types of data considered sensitive.[16] Often, due to the patchwork of regulations, there are conflicts between regulations. Even within the same sector of data there are different regulations and standards. For instance, in the health sector there is: the Health Insurance Portability and Accountability Act ("HIPPA") which is the primary health and security privacy law, the Family Educational Rights and Privacy Act ("FERPA") which deals with student immunization and school health records, and Children's Online Privacy Protection Act ("COPPA") which only protect data for children under thirteen years of age.[17]

Most of the states have adopted breach notifications laws, however, how and who the company must notify varies from state to state. For example, New Jersey requires that the State Police Cybercrime Unit to be notified, whereas Maryland requires the State Attorney general be notified before any other individual.[18]

d) Countries with the Worst Privacy Protection and Extensive Surveillance of Their Citizens

Comparitech, a consumer protection focused website, conducted an assessment out of 47 countries to evaluate on privacy protection and surveillance, scoring them from 1-5 (5 being the best and 1 the worst). The assessment found that the top five countries with the

[16] Digital and Cyberspace Policy Program, "Reforming the U.S. Approach to Data Protection and Privacy," Council on Foreign Relations, (January 30, 2018), available at: https://www.cfr.org/report/reforming-us-approach-data-protection
[17] *Id.*
[18] *Id*

worst privacy protection and extensive endemic surveillance were: China, Russia, India, Thailand, and Malaysia.[19] Following is an explanation on why experts have found China to lack in digital privacy rights protections.

The Comparitech assessment found that despite China having privacy laws, the laws lack guidance and therefore difficult to enforce.[20] Some of the concerns expressed by Comparitech were: State practices sharing personal data among agencies; there is no legislation on how long personal data can be stored, yet there are specific guidelines on what data needs to be stored by state and non-state actors; and data recollected for medical reasons are often misused under the guise of "public interest records."[21] While the lack of data protection is used for state surveillance it has also contributed for the easily accessible data to be misused by individuals for private extortion and fraud.[22]

It is important to note that in late 2018, China announced it placed personal data protection legislation on the agenda and on June 2019 the government released a set of guidelines to be followed by different mobile apps.[23] The guidelines were regarding informed user consent and what information can be accessed by the mobile apps. Although it does not solve the privacy issue, it a start towards comprehensive legislation. Concern has been expressed on whether the government will enforce this temporary regulation.[24]

---

[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] Feng, Emily, "In China, A New Call To Protect Data Privacy," NPR, (January 5, 2020), available at: https://www.npr.org/2020/01/05/793014617/in-china-a-new-call-to-protect-data-privacy
[23] Ma Wenyan, Wiston, "China is waking up to data protection and privacy. Here's why that matters," World Economic Forum, (November 12, 2019), available at: https://www.weforum.org/agenda/2019/11/china-data-privacy-laws-guideline/
[24] *Id.*

III. Gender Based Perspective to Privacy Rights

According to European Digital Rights ("EDRi"), an association of civil and human rights organizations from Europe, new technologies tend to reinforce societal biases.[25] As a result, vulnerable populations such as women and LGBTQ people are more vulnerable to "discrimination and security threats."[26] Although technologies have helped promote and advocate for human rights, technology does not operate in a neutral way. Some services and apps have shown a "heteronormative and gender-biased nature."[27]

a. Women and LGBTQ People

There are several ways women and LGBTQ people are impacted by the lack of or insufficient digital privacy rights protection. When there is a lack of privacy rights, women and LGBTQ people are more likely to suffer gender based violence. The violence suffered by both group of people can range from online harassment and blackmail to physical stalking and abuse. The organization Privacy International, states that the lack of online privacy laws have heightened the degree of abuse that survivors of online gender-based violence have gone through. Online gender-based violence is not an isolated occurrence because often the violence mirrors what happens in society. Survivors of online gender violence have described their ordeal as "impossible to escape" because technology has made the physical world and the online world inseparable.[28]

---

[25] Berthélémy, Chloé, "The Digital Rights of LGBTQ+ People: When Technology Reinforces Societal Oppressions,"EDRi, (July 17, 2019), available at: https://edri.org/the-digital-rights-lgbtq-technology-reinforces-societal-oppressions/
[26] *Id.*
[27] *Id.*
[28] "#IWD2019 Online gender-based violence: a privacy matter?," Privacy International, (March 7, 2019), available at: https://privacyinternational.org/long-read/2760/iwd2019-online-gender-based-violence-privacy-matter

Privacy issues often have different consequences and manifest in different circumstances for women. For instance, a study conducted by the Pew Research Center, a nonpartisan fact tank that asses global issues, attitudes, and trends, found that women are more likely to be sexually harassed online.[29] Victims of online harassment have experience physical consequences "ranging from mental or emotional stress to reputational damage or even fear for one's personal safety."[30]

To address the problem of digital privacy over of these vulnerable populations, States need to imbed a gender perspective not only when legislating on data protection, but also on the implementation and enforcement of those laws.[31] To be able to utilize a gender perspective in the implementation of policies and guidelines it is necessary to interpret the content of certain provisions from a woman's or queer person's point of view. Privacy international suggest that the policies and guidelines should require "the need for an explicit, freely given and unambiguous consent; legitimate interest of a data subject when they are woman or queer persons; or to ensure the necessity for data processing for a contract."[32]

i. Non-Consensual Image Sharing (Revenge Porn)

An emerging problem that States have rarely address is revenge porn, also known as doxing. Revenge porn is when a person's intimate videos or photos are sent to a sexual partner with the implied agreement that those would not be shared or shown to third

[29] See *supra* note 14.
[30] Duggan, Maeve, "Online Harassment 2017," Pew Research Center, (July 11,2027), available at: https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/
[31] "Privacy International's submission on the consultation 'Gender perspectives on privacy,' Privacy International, (September 2018), available at: https://privacyinternational.org/sites/default/files/2018-11/PI%20submission%20on%20gender%20consultation_September%202018.pdf
[32] *Id.*

parties, but one of partner's decide do make the image or videos private when the relationship ends or because of a perceived transgression by the other. This practice is used to "oppress women and gender diverse people."[33] The majority of States around the world do not have a doxing law. The current countries with revenge porn laws are England, Wales, Scotland, Northern Ireland, Malta, Germany, France, Australia, Canada, Philippines, Israel, and Japan.[34]

When addressing revenge porn privacy law, the problem is more complicated because it is no longer an issue of adding a gender perspective, but one of lack of legislation entirely. Furthermore, even when there are laws in place, often times police do not investigate cases diligently nor do courts enforce the law properly when there is a law in place.[35] When a victims files a lawsuit or requests an investigation, they are usually revictimized in the process because of improper police and judicial work which has allowed abusers to go consequence free. Utilizing a gender perspective would serve the victims of these privacy violation in ultimately getting justice for the harm done to them.

IV. Conclusion

Digital data privacy is a prevalent issue today. Data privacy encompasses many aspects such as: security and surveillance; big data and open data; health data, and the use of personal data by state and non-state actors. In the absence of clear legislation and effective

[33] *Id.*
[34] "Revenge Porn Laws Across the World," The Center for Internet & Society, (April 25, 2018), available at: https://cis-india.org/internet-governance/blog/revenge-porn-laws-across-the-world
[35] *Id.*

enforcement, individuals' information is at risk of being improperly used, collected, and access which could lead to extortion, fraud, and overreaching surveillance.

Regarding the need for a minimum standard of care for the protection of digital privacy rights HRA recommends that the Human Rights Council:

1) Ask States to make data protection and cybersecurity a priority;
2) Ask States to create comprehensive domestic legislation to protect privacy rights online; and
3) Call for a universal global legislation on data protection and cybersecurity.

Regarding the need digital privacy right protection for vulnerable populations HRA recommends that the Human Rights Council:

1) Ask States to recognized that societal biases and prejudices present in society are also present online and must therefore create legislation to protect vulnerable groups; and
2) A gender perspective be adopted in the legislation, implementation, and enforcement of privacy laws.