2021

A Review of Data Protection Regulations and the Right to Privacy: the case of the US and India

Chrisann Campbell
CUNY City College

A REVIEW OF DATA PROTECTION REGULATIONS AND THE RIGHT TO PRIVACY: THE CASE OF THE U.S. AND INDIA

Chrisann Nateish Campbell

MASTER'S THESIS

Submitted in Partial Fulfillment of the Requirements for the Degree of Master of International Affairs at the City College of New York

COLIN POWELL SCHOOL FOR CIVIC AND GLOBAL LEADERSHIP

Advisor: Professor Kimberly Gamble-Payne

Second Reader: Professor Jean Krasno

Contents

Acronym

CCPA	California Consumer Privacy Act
DHS	Department of Homeland Security
DPAI	Data Protection Authority of India
EU	the European Union
FIPPS	The Fair Information Practice Principles
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
HEW	Department of Housing, Education & Welfare
HIPAA	Health Insurance Portability and Accountability Act
IAMAI	The Internet and Mobile Association of India
IOM	International Organization for Migration
NPI	Non-Public Information
NPR	National Public Radio
OAS	Organization of American States
APEC	Asian Pacific Economic Cooperation
OECD	The Organization for Economic Co-operation and Development
PDP	Personal Data Protection Bill
PHI	Protected Health Information
PII	Personal Identifiable Information
U.S.	United States

Abstract

Since 1948 and the signing of the Universal Declaration of Human Rights, the concept of privacy has grown more complex with the rise of technology and a shift to the internet. In particular, the unregulated use of technologies that can capture individual's personal data without their knowledge or consent poses a threat to their right to privacy and other additional human rights. The protection of the collection, storing, and transfer of users' personal data against data breaches also ensures that the right to privacy is guaranteed. Through examining two countries, the U.S. and India, on the idea of privacy, personal data, and data protection, I hope to provide an insight into the ongoing issues in each country on their path to adopting comprehensive data protection legislation. I will use the European Union General Data Protection Regulation as the standard to which each country should uphold as an adequate data protection regulation. What do the case studies on each country provide on the perception of data protection and the right to privacy? This paper suggests a convergence of interest among all countries in adopting a national data protection legislation which resembles that of the EU General Data Protection Regulation. However, different aims and interests of nation-states prevent the adoption of adequate data protection, which protects privacy.

Chapter I: Background on Research

The most comprehensive and impactful legislation concerning the protection of personal data can be found in Europe. In the Charter of Fundamental Human Rights of the European Union (CFR.), a legally binding resolution, Article 8 explicitly states that one has the right to protect their personal data, and have it processed soundly.[1] Essentially, data protection has been designated a fundamental human right in the European Union. Data protection regulations are now thought to be one of the most critical issues that need to be addressed as we move to the age of Big Data. With the rise of technology and globalization, people's names, social media accounts, and sometimes highly sensitive online information are being sold and transferred across borders through our screens. Along with the rise of cyber warfare and terrorism, unwanted surveillance, and collecting people's personal data without proper data protection regulation, the right to privacy is at risk.

In a 2021 *Data Breach Investigation Report* (DBIR) by Verizon, one of the largest wireless carriers in the United States, about 5,258 data breaches were confirmed to have taken place in over 88 countries with 79,635 incidents reported instances in 2020.[2] Data breaches, defined by the report, are security incidents where confidential data is seen as being compromised.[3] In 2013, the most severe data breach reported was the Yahoo Inc. incident, which exposed three billion customer accounts, with another breach affecting 500 million users reported shortly after.[4] The incident involved hackers, some later arrested, accessing customers' email accounts, including their names, email addresses, telephone numbers, birth dates,

[1] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, available at: https://www.refworld.org/docid/3ae6b3b70.html [accessed 19 December 2020]
[2] "2021 Data Breach Investigations Report." Verizon Enterprise. Accessed March 21, 2021. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf,6.
[3] Ibid,22.
[4] Nicole, Perlroth, "All 3 billion Yahoo Accounts Were Affected by 2013 Attack." The New York Times. October 03, 2017. Accessed December 20, 2020. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

passwords, and answers to security questions. Both incidents have since prompted a settlement from Yahoo totaling about 117.5 million to customers and shareholders. It was also reported that Yahoo failed to own up to the incident, tried to diminish how significant the incident was, and failed to have adequate network security and only did so when the company was going to be sold to Verizon in 2016.[5] According to a New York Times report on the incident, in 2016, yahoo users' account information later started selling on the dark web, a hotbed for criminals.[6]

With the failure to protect users' account information, fraud and identity information can destroy ones' livelihood and ruin the image of a company. About 16 billion dollars was reported stolen from victims of identity theft in 2020.[7] It is also common for victims to go unaware of data breaches, and often time breaches go unnoticed.[8] In 2017, the United States faced another breach from its credit bureaus, Equifax, where people's social security numbers, names, birth dates, addresses, and driver's license information were exposed. According to IBM's *Cost of a Data Breach Report 2020*, businesses not only lose trust in their customers, but cost businesses 3.86 million dollars on average each year.[9] In the United States, that cost skyrockets to 8.64 million dollars a year.[10] The increased expenses on the companies include the cost of legal fees,

[5] Ping, Wang and Sun-A. Park. "COMMUNICATION IN CYBERSECURITY: A PUBLIC COMMUNICATION MODEL FOR BUSINESS DATA BREACH INCIDENT HANDLING." Issues in Information Systems 18, no. 2 (2017),142.
[6] The dark web is described in the Congressional Report R44101 as "content that has not been indexed by traditional search engines such as Google." It is generally used for unlawful purposes by criminals to sell or obtain content.
[7] Kelligrant. "Identity Theft, Fraud Cost Consumers More than $16 Billion." CNBC. February 01, 2017. Accessed June 18, 2021. https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html.
[8] The Council of Economic Advisers. 2018 The Cost of Malicious Cyber Activity to the U.S. Economy. Washington, DC: Executive Office of the President, 2018,33.
[9] "Cost of a Data Breach Study." IBM. Accessed June 18, 2021. https://www.ibm.com/security/data-breach.
[10] Ibid.

settlements, cost of improving security measures, regulatory penalties, increased public relations to fix reputable damages, and resources used to notify customers of such breaches.[11]

As the internet age progresses, more and more people use the internet to conduct transactions, communicate, track their credit score and join social media. The internet age has brought everything to our fingertips, but companies are also more at risk of not only being hacked but failing to protect the information of their users. No more so than ever, there are concerns over privacy and the lack of data protection provided by companies and governments alike. In 2018, the European Union adopted the most stringent data protection policy known as the General Data Protection Regulation (GDRP). These regulations have prompted the larger international community to regard data protection as a right in an increasingly digitized world. Furthermore, with the rise of international standards on data protection such as the *U.N. Principles on Personal Data Protection (2018) & Privacy*, ASEAN *Framework on Personal Data (2016), and APEC Privacy Framework (2015*), Interpol's *Int'l Criminal Police Org., Rules on the Processing of Personal Data (2016) U.N. High Commissioner for Refugees, Policy on the Protection of Personal Data of Persons of Concern to UNHCR (2015),* the international community has called to create an international framework in order to address privacy and data protection, with the EU's GDPR as the main framework. [12]

Purpose of the Study

This paper aims to examine the two case studies of the United States and India to show that they do not have adequate data protection regulations to provide the right to privacy and suggest ways that these two countries may move further towards the path of adopting adequate

[11] The Council of Economic Advisers. 2018 The Cost of Malicious Cyber Activity to the U.S. Economy

[12]Christopher, Kuner, "An international legal framework for data protection: Issues and prospects." Computer law & security review 25, no. 4 (2009), 307.

data protection rules. The United States is the largest economy, the most affected by data breaches, but most importantly, along with China, a leader in the digital age. On the other hand, India is a leading emerging country where only half of the population has internet access. Both countries are not only two of the largest democracies, but each also ranks number one in the Global Innovative Index in their respective regions, North America and Central and Southern Asia. The index model measures each country's ability to innovate into new tech, investment, research, and other metrics that may affect the economy.

Definitions and Terminology

Every day, countless consumer information is collected by companies and organizations. It is not only what companies do with this information that is a concern but also the lack of information protection. Such information often includes what is referred to in the U.S. as personal identifiable information (PII)**.** For the U.S. Department of Labor, personal identifiable information is defined as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." [13] Examples include social security numbers, driver's licenses, bank accounts, addresses, and phone numbers. Not only is this a concern in the private sector but also the public sector with the mass data gathering by governments of nation-states of their own people. In comparison, article 4 of the European Union General Data Protection defines personal data as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, 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.[14]

[13] "Guidance on the Protection of Personal Identifiable Information." U.S. Department of Labor Seal. Accessed June 18, 2021. https://www.dol.gov/general/ppii.
[14] "What Is Considered Personal Data under the EU GDPR?" GDPR.eu. February 13, 2019. Accessed June 06, 2021. https://gdpr.eu/eu-gdpr-personal-data/.

The European definition is generally thought to be the broader of the two. It goes beyond information that can directly lead to the identification of a person, such as their name and credit card information, birth date, social security number, passport number, and Health insurance ID number. The EU definition expands this list to include data that can *indirectly* lead to someone's identity, such as their Internet Protocol (IP) address or other cultural and social factors such as religion or political affiliation or mental illness and social media posts. Lastly, other types of personal information similar to GDPR has been introduced into the California Data Protection Act (CCPA). Personal information is defined in the CCPA as:

> information that identifies relates to or could reasonably be linked with you or your household. For example, it could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.[15]

Subsequently, the use of different terminologies and definitions also means that there are disagreements between some of the most prominent countries and what they deem as information that should be protected. We shall see this in the case of the U.S. Privacy Shield.

The processing of personal data is one of the primary sources of economic growth.[16] Scholars have dubbed personal identifiable information "the new oil."[17] Knowledge that is gained from the personal information is a driver of economic growth and corporate profit. Personal data is now the source of fuel, often manipulated into data trends or consumer behavior

[15] "California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General. July 14, 2021. Accessed July 20, 2021. https://oag.ca.gov/privacy/ccpa.
[16] Ibid.
[17] "The World's Most Valuable Resource Is No Longer Oil, but Data." The Economist. May 6, 2016. Accessed May 01, 2021. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

analytics by companies that leads to the production of new products and personalized advertising. The use of servers, computer software that connects via the internet has provided a vacuum to storing and collecting personal data in what is regarded as a data-driven society. Large volumes of data are stored and processed as a "resource for driving value creation, fostering new products, processes, and markets, as well as enabling the creation of new knowledge."[18] Thus, privacy concerns stem from the volume, velocity, and variety of data where companies not only fail but are not even required to protect personal data from unauthorized access. The collection also poses privacy concerns as to just how much information companies are gathering and whether they are allowed to collect this information.

I argue that national data protection regulations would change the way businesses handle personal data. Privacy and data regulations would also give back some autonomy and control to users about how personal data is collected and processed, such as requiring consent first from consumers before companies are able to process data. Comprehensive data protection like the General Data Protection Regulations binds businesses and organizations to obligations such as (1) ensuring data security mechanisms, (2) promoting transparent business practices about the use of personal data (3) protecting data providers' rights, (4) requiring data protection officers to be in place to ensure that expectations are met, and (5) imposing penalties. Data protection regulations also establish a set of rights for data providers and data users.

[18]Sonja Zillner, Tilman Becker, Ricard Munné, Kazim Hussain, Sebnem Rusitschka, Helen Lippell, Edward Curry, and Adegboyega Ojo. "Big data-driven innovation in industrial sectors." In New Horizons for a Data-Driven Economy, (2016) pp. 167.

Chapter II: Literature Review

The oldest record of data protection regulation can be found in Europe in Germany, in the city of Hesse in the 1970s, followed by the Data Act in Sweden over concern on personal data and computing. Directly across the pond was the creation of the Fair Information Practice Principles or FIPPs, as a set of principles introduced in the United States that would form the foundation and backbone for regulations created to address the use and handling of personal information. The FIPPS emerged from the Department of Housing, Education & Welfare (HEW) advisory committee on the risks to privacy posed by the growing technological world. The principles outlined addressed transparency, use limitation, access and correction, data quality, and security in the digital space. They aimed to provide individuals with the ability to engage in their personal data being collected by being informed when it is happening. The Fips were to become the gold standard for protecting personal information and have been regarded as the basis for much of U.S. privacy and data protection laws and influencing broader international regulations, as we shall see. However, many of the literature reviews on the Fips all agree that they have failed to make much difference in collecting personal data in the United States.

Another critical initiative on data protection was the *Convention for the Protection of Individuals concerning Automatic Processing of Personal Data* or the European Convention 108. It was one of the first to address the protection of individuals "against abuses which may accompany the collection and processing of personal data, and which seeks to regulate at the same time the transfrontier flow of personal data." [19] Convention 108 was formed from the Council of Europe (CoE), who were fearful of the extent to which public authorities had access

[19]Council of Europe, Convention for the Protection of Individuals concerning the Automatic Processing of Individual Data, 28 January 1981, ETS 108, available at: https://www.refworld.org/docid/3dde1005a.html [accessed 19 December 2020

to citizens' private life. In 1981, the legally binding treaty was signed with over 55 signatory members. Though it was formed under the Council of Europe, a voluntary international organization of ministers of foreign affairs whose aim was to cooperate on human rights and democracy in Europe, Convention 108 welcomes any country to become a signatory member. Outside of the EU member states, eight other non-EU member states have joined this treaty, while countries like the U.S. and Canada remain observatory members. As it stands, India is currently ineligible as it has yet to adopt a comprehensive data protection regulation.

In the 1990s, the EU Directive became another vital tool in Europe in the transmission of personal data across borders. The Directive is also regarded as a predecessor of the new E.U. General Data Protection Regulation (GDPR), signed in 2018, is considered the strictest privacy and security law. While meant to standardize the flow of personal information, including storing, transmitting, and processing EU member states, the Directive also placed the exact expectations and guaranteed protections of EU citizens when their data flowed from outside the EU. This meant that non-member EU states had to comply with the Directive to receive any data transfer from European living within their borders. Furthermore, the Directive also explicitly entailed that companies ensure that European citizens' rights to privacy and processing of their personal data, both fundamental rights, were protected.[20]

In 1981, the Organization for Economic Co-operation and Developments' (OECD) issued the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* the same year of the CoE Convention 108. The Guideline is currently the only internationally agreed-upon global framework on data protection law that has been successful in being adopted into multiple national legislation such as Australia's Privacy Act of 1988, New Zealand's Privacy Act of 1993

[20] Privacy as a theoretical concept, 199.

and was even used as a foundation when Canada's started working on their data protection laws, later known as PIPEDA.[21] Previously named, Organization for Europe Economic Co-operation (OEEC), the OECD was designed to help Europe after WWII with the Marshall Plan and foster economic interdependence. Its primary mission includes advising and promoting "international standard-setting" policies regarding the economy and societal standards to its member states.[22]

The Guideline was drafted mainly due to the lack of standardization of personal information processing and data transfers. Additionally, the Guideline set out to ensure that there would be no barriers to global economic activity due to the rise of privacy laws.[23] The regulation sets out a set of principles to be implemented by the OECD member states, such as collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[24] The goal of these principles is also to promote a sense of transparency about transferring personal data while promoting a sense of privacy.[25] The OECD framework and Convention 108 share many similarities being that they came out during the same year and shared principles. The OECD has been said to be an inspiration from Convention 108. The Guidelines have since been updated in 2013 with no changes made to the original principles but the "privacy management programmes" now includes adopting a breach notification policy, performing risk assessments on potential risk factors, in anticipation of any unauthorized access.[26] There is also a call for adopting legislation at a more coordinated level, meaning that multiple agencies and levels of Government work together to form legislation that does not class with other agencies or matters of Government such as national security.

[21] Ibid,77.
[22] Organization for Economic Co-operation and Development. 2013, "The OECD Privacy Framework." https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, 116.
[23] Ibid.
[24] Ibid.
[25] Ibid
[26] Ibid.24.

The United Nations has also begun playing a role in promoting data protection regulations. In 1990, they also adopted the United Nations Guidelines Concerning Computerized Personal Data Files. In 2015, The United Nations Human Rights Council also appointed a Special Rapporteur to the right of privacy in response to globalization, the rise of big data, and surveillance practices by governments that may violate privacy rights. The Rapporteur role includes critiquing national policies on collecting personal data, privacy and ensuring that the laws comply with the international standards on the respect of human rights obligations.

Privacy and Personal Data

According to the European Union Data Protection Supervisor, Wojciech Wiewiórowski, whose primary responsibility is to ensure compliance among the European institutions on the GDPR, privacy and data protection go hand in hand when maintaining a "sustainable democracy."[27] The Universal Declaration of Human Rights treaty signed in 1948 represents a universal agreement on the fundamental human rights that everyone should enjoy. Additionally, it is codified in Article 17 in the International Covenant on Civil and Politics Rights of 1976 as a legally binding document, in the Charter of Fundamental Human Rights of the European Union in Article 12 as well European Convention on Human Rights in article 8 and the American Convention on Human Rights in article 11.

Privacy itself is a contested terminology and is said to be mentioned as early as in the Bible.[28] It is often said to encompass many things, but there remains a debate among scholars on what it means. In conceptualizing privacy, Professors Leslie P. Francis and John G. Francis denote that there is no one meaning of privacy related to various aspects/assets of an individual's

[27] Data Protection." European Data Protection Supervisor - European Data Protection Supervisor. November 11, 2016. Accessed October 20, 2020. https://edps.europa.eu/data-protection_en.
[28] Global Trends in Privacy Protection: An International Survey of privacy, 6.

life, and other freedoms are guaranteed through privacy. Privacy is thought to be intrinsic to other rights such as freedom of religion, freedom of expression, and the right to life and liberty. Researchers often point to "T*he Right to Privacy*," an article published in 1890 by American lawyers Warren and Brandeis who advocated for recognizing the right to privacy in the United States Constitution and the definition of "the right to be let alone."[29] Similarly, the EU defines privacy as the right to a private sphere where no one can interfere and where specific information about a person belongs to them alone, and they are in control of what happens to it. [30] Often the right to privacy has to do with the private sphere versus the public sphere. However, as Special Rapporteur Eli Frank writes, the internet of things has changed the way we communicate and has "irreversibly affected our understandings of the boundaries between private and public spheres."[31]

Professor of Law Roger Clarke defines privacy as the "integrity of an individual, "and provides five subsets to privacy: Privacy of the Person, Privacy of Personal Behavior, Privacy of Personal Communications, Privacy of Personal Data, and more recently, Privacy of Personal Experience.[32] Privacy of Data deals with the protection and the autonomy over the data dealing with an individual, which he refers to as data privacy or informational privacy.[33] Privacy of an individual thus can mean many things like their property where they can deny entry on their personal property; privacy in terms of saying no to be searched or what to do with one's body;

[29]Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Skorvanek, Tomislav Chokrevski, and Masa Galic. "A typology of privacy." U. Pa. J. Int'l L. 38 (2016): 548.
[30]Shraddha Kulhari, "Data Protection, Privacy and Identity: A Complex Triad." In Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity, 23-37. Baden-Baden, Germany: Nomos Verlagsgesellschaft MbH, 2018, 23.
[31] Frank, La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Report to the United Nations General Assembly." Human Rights Council. A/HRC/23/40 (2012), 6.
[32]Bert-Jaap Koops, "A typology of privacy.",498-499.
[33] Ibid, 499.

keeping one's personal data private, and the right to communicate freely and privately on emails and social media.[34]

How then do we ensure the protection and the right to privacy? Bernhard Debatin outlines three ways. One way is through legal regulation such as adopting a comprehensive data protection regulation and recognizing privacy in such things as a national constitution. The second way is through ethical self-regulation, which uses the adoption of rules which intimately become norms and expected behavior in "institutions that typically deal with any kind of personal information."[35] Lastly, the development of privacy-enhancing techniques such as firewalls, spyware detectors, data encryption, and anonymization tools help to ensure additional protection of data management systems and prevent these systems from being accessed by outsiders.

Privacy and Data Protection

Privacy and data protection are often misconstrued as being synonymous. However, they are distinctly recognized as different fundamental rights in the Charter of Fundamental Human Rights of the European Union. For many other countries outside of the EU, privacy and data protection are often lumped together and are used interchangeably as data protection is not a fundamental right outside of the EU. For some researchers, data protection regulations are seen as a subset of privacy since it may be inferred that protecting one's personal information is privacy itself. Data protection serves to protect the right to privacy since personal data is considered belonging to or part of a person's identity. According to Kulhari, privacy is a concept

[34]Shraddha Kulhari, "Data Protection, Privacy and Identity: A Complex Triad." In Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity, 23-37. Baden-Baden, Germany: Nomos Verlagsgesellschaft MbH, 2018, 23.
[35] Bernhard Debatin "Ethics, Privacy, and Self-Restraint in Social Networking" In *Online: Perspectives on privacy and self-disclosure in the social web*, eds. Trepte, Sabine, and Leonard Reinecke, (Springer Science & Business Media, 2011),49.

associated with "personhood and identity," thus, data protection encapsulates these self-determination ideas."[36]

The Organization of American States (OAS) compares the relationship between the right to privacy and data protection to the ranking of biological classification such as the genus and a species. In taxonomy, the genus is the rank of the grouping of similar organisms or species with similar attributes. Data protection thus serves as a species whose aims relate to protecting the fundamental right to privacy, especially those whose personal information is in danger of being exposed or access by those unauthorized to access it. The International Organization of Migration (IOM) Data Protection Manual expands the definition of data protection to "the systematic application of a set of institutional, technical and physical safeguards that preserve the right to privacy with respect to the collection, storage, use and disclosure of personal data."[37] For Paul De Hert and Serge Gutwirt, data protection is a "tool of transparency" in that it aims to make sure others are aware of how their persona data is being processed and that organization is held to a standard in which they ensure that users personal data is not at risk of being exposed. Data protection thus serves to ensure accountability, transparency, and protection when it comes to the processing of personal data. Data Protection is also known as information privacy, data privacy as interchangeable words, and throughout this paper, I will use these terms synonymously.

Approaches on Data Protection Regulation

A global landscape on data protection regulations designed to protect consumer rights has emerged within the last ten years with the adoption of national regulations. In 2011, there were

[36]Shraddha Kulhari, 26.

[37]International Organization of Migration. The IOM Data Protection Manual, 2011, statement. Switzerland: International Organization of Migration, 2011.

only 76 countries that had enacted data privacy laws, and by 2019, that number had increased to 132 countries.[38] In one year, from 2017-2018, data privacy laws rose from 120 to 132 to constitute the most significant percentage increase of 10%.[39] According to Greenleaf, a professor of Law & Information Systems in Australia and a well-known scholar, many of these countries have adopted this legislation to adhere to the regulations set under the GDPR. There is also a consensus that a data protection regime will protect consumers' rights in a global economy

According to the United Nations Conference on Trade and Development (UNCTAD), about 128 countries to date have a national data protection law.[40] That is also about 66% of the 194 countries, all of which are United Nations member states. Of the least developed countries (LDCs), about 26 already have legislation or are currently working on draft legislation to address data protection and privacy.[41] The Asia-Pacific countries have the lowest percentage of adoption of legislation concerning data protection and privacy to date.[42] However, adopting privacy and data protection regulations does not equate to having proper mechanisms to protect our privacy.

Aside from the EU GDPR, other important data protection legislation that has been adopted or updated around the world to address includes Canada's PIPEDA, Japan's Act on Protection of Personal Information, Thailand Personal Data Protection Act (PDPA), and more recently, Brazil's Lei Geral de Proteçao de Dados (LGPD) and China Personal Information Protection Law of the People's Republic of China (PIPL). These countries have all adopted an omnibus bill. Rather than an overarching federal regulation, the U.S. has depended on sectors to create their own rules and regulations about protecting privacy. Even the ones passed in

[38]Graham Greenleaf, "Global data privacy laws 2019: 132 national laws & many bills." 157 Privacy Laws & Business International Report. February 8, 2019, 14.
[39] Ibid.
[40] "Data Protection and Privacy Legislation Worldwide." UNCTAD. Accessed April 01, 2021. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.
[41] Ibid.
[42]Ibid.

Congress are "unfair and deceptive."[43] Similarly, data protection regulations that have emerged have been omnibus laws often where privacy is explicitly stated in their constitution, and regulations often cover a wide-ranging number of sectors and organizations together. Countries like the U.S. does not explicitly have a right to data privacy in their constitution. In these cases, interpretations are used to determine laws regarding what values like privacy and data protection equate to. Those can be different depending on the relationship that the government has with sectors. Among scholars, there is a consensus that a holistic approach and adopting an omnibus approach to data protection and privacy is desired to address globalization's growing nature.

The Challenges to Data Protection Regulations

Multiple factors challenge the progress of the ongoing data protection regime. Data Protection requires two parts, a legal framework and technical standards. Regulations are often complex as it affects society, economic development, and national security. On the one hand, data protection legislation poses a challenge to lessen data flow in a world driven by data analytics. On the other hand, it poses a positive change to increase consumers' trust and increase innovations that could provide possible safeguard personal data.[44] According to Raymond Wacks, data protection regulation only sprung up not in response to big data but for the so-called common good.[45] It was in part seen as necessary and in the interest of humanity for data protection regulation to exist to prevent the misuse of personal and give people a say in how they would share this information. More importantly, privacy is not an absolute right. The right to privacy is often said to conflict with national security, which also tends to trump the right to

[43] U.S. Congressional Research Service. Data Protection Law: An Overview (R45631; March 25, 2019). Text in LexisNexis® Congressional Research Digital Collection; Accessed: November 20, 2020, 69.
[44]Crispin Niebel, "The impact of the general data protection regulation on innovation and the global political economy." Computer Law & Security Review 40 (2021),12.
[45] Page 106, Raymond Wicks, Privacy a concise introduction.

privacy as often "many jurisdictions, intelligence and law enforcement agencies are excluded from the provisions of data privacy legislation." [46] Particularly cases such as 9/11 and the Patriot Act are cases where national security meant giving up the right to privacy in exchange for protection.[47] Privacy laws have often clashed with national security matters and laws allowing surveillance, fingerprints on ordinary citizens, and collection of personal data. Some of these surveillance activities have been judged to be undemocratic.

In July 2020, the European Union Court of Justice invalidated the EU-US Privacy Shield declaring that the framework was insufficient to its own EU level of protection required to transfer personal data from the European Union to the United States. This framework was meant to ensure that the U.S. met the standards needed, but it was not enough for the EU. A similar event occurred to its predecessors, the International Safe Harbor Privacy Principles, in October 2015. More importantly, the U.S. could lose up to 7.1 billion dollars because of the invalidation of the shield.[48] This is just another example of the challenges to data protection as a lack of coherence of regulations and harmonization of data privacy laws exist across regions, putting pressure on economies that depend on data sharing and international cooperation. Also applicable to this, as stated earlier, a region or country has different definitions of personal data and applies contrasting rules that deal with the processing of information.

Another challenge is the increased use of artificial intelligence. The use of supercomputers and algorithms means billions of data are being processed faster and making better predictions and inferences.[49] Artificial intelligence can be used to track, identify and

[46] United Nations, Office of the High Commissioner for Human Rights. The right to privacy in the digital age: report (3 August 2018). available from https://undocs.org/A/HRC/39/29,10.
[47] Ibid.
[48] "Factbox: Reaction after EU Court Strikes down Transatlantic Data Transfer Deal." Reuters. July 16, 2020. Accessed May 01, 2021. https://www.reuters.com/article/us-facebook-privacy-eu-reaction-factbox/factbox-reaction-after-eu-court-strikes-down-transatlantic-data-transfer-deal-idUSKCN24H1QV.
[49]Manon Oostveen, and Kristina Irion, 15.

surveil individuals on devices that use AI technology. AI technology can be harmful as humans create algorithms that can be biased, and as such, AI can produce harmful and unlawful decisions used by organizations. These decision-making machines can target people and groups, allowing for profiling and thus discrimination against rights protected under national legislation. The other issue with AI technology is the lack of transparency around the processing of data. AI technology increasingly requires more and more data that users may be unaware of being used or collected and can infringe upon the right to privacy and data protection regulations.[50]

Influence of Europe's Data Protection Laws

In 2011, there were only 76 countries that had enacted data privacy laws. By 2019, that number had increased to 132 countries.[51] In one year, from 2017-2018, data privacy laws rose from 120 to 132 to constitute the most significant percentage increase of 10%.[52]. According to Greenleaf, a professor of Law & Information Systems in Australia and a well-known scholar, countries have adopted this legislation to adhere to the ruling of the GDPR and move towards an international standard on regulations.

In a much earlier report in 2012, Greenleaf coined the term “European Elements” when he compared the EU Directive and the Council of Europe Convention 108 against the OECD Guidelines and APEC Framework. Of 39 non-EU states, 33 examined by Greenleaf have adopted what he coined the 10 "European elements" to data privacy laws. Also, at least 13 states had 9/10 of the elements.[53] The author lays out that countries like the U.S. and China are "outliers" to this phenomenon.[54] Greenleaf writes that the U.S. position on data privacy law

[50]Ibid,17.
[51]Graham Greenleaf, "Global data privacy laws 2019: 132 national laws & many bills." 157 Privacy Laws & Business International Report. February 8, 2019, 14.
[52] Ibid.
[53] Graham Greenleaf. "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108." International Data Privacy Law 2, no. 2 (2012): 2011-39,12.
[54] Ibid, 3.

makes them unique. They have rules here and there, some sector-based rules rather than comprehensive ones; some are strict, and others that are weak against security breaches leave nothing to be desired. This pits them against a growing network of states requiring stricter data privacy rules from countries where much of the "internet-based" services originate.[55]. With non-EU states adopting some of these "European elements "in their national policies, the EU exercises its soft power and plays a significant role in norm sharing.[56]

Like Greenleaf, professor of law at the Tel Aviv University, Michael Birnhack's study on the EU Data Protection Directive, the predecessor to the GDPR, and its global impact concludes that the EU is pushing for a "global data protection regime."[57] A survey of before and after states interacting with the EU by the way article 25 "allows transfer of data to a third country only if the third country ensures an adequate level of data protection," is completed. He concludes that countries that wish to engage in data transactions with EU member states are forced to align their policies, thus indirectly raising their own domestic data privacy laws.[58]

[55] Ibid, 6.
[56] Ibid, 34.
[57] Michael D Birnhack. "The E.U. Data Protection Directive: An engine of a global regime." Computer Law & Security Review 24, no. 6 (2008): 508.
[58] Ibid.

Chapter III: Methodology

The literature review aimed to show how vital data protection is in an age where the issue of privacy has become a central issue. Data protection and privacy legislation together create the opportunity to address data governance. The above literature review has shown that privacy and data protection are intrinsic to one another. In the current climate of massive volumes of data collection, privacy cannot exist without a data protection policy. The role of data protection is not to stop the flow of data but to provide safeguards for individuals against their personal data being abused. Data protection ensures that there is informational privacy.

Based off the literature review, I make some assumptions and inferences to set up a comparative analysis. First, data protection advocates can agree that privacy and data protection are engrained in each other as we cannot have privacy without security. Under European law, everyone has a right to have their personal data protected. And safeguarded against intrusion. The ones who provide this security are the organizations and companies that collect our personal information. Secondly, as discussed earlier, what is personal data varies across organizations, countries, and regions, as does the concept of privacy. Thus, countries will take varying approaches to data protection regulations.

This chapter will aim to discuss the approach that the EU took in its handling of privacy and what makes the GDPR an adequate data privacy ruling. This will help later when comparing the other data privacy initiative by the case studies. The General Data Protection Regulation is still relatively new as it marked its third anniversary in October 2021. Yet research suggests there is a proliferation of a European standard that can be seen from Europe's earlier legislation, the EU Directive, and as Greenleaf describes in the previous chapter, the GDRP is inspiring sweeping legislation across the globe through what is described in International Relations as the

Brussels effect. The EU has utilized its economic and soft power capabilities to socialize where "states internalize norms originating elsewhere in the international system."[59]

EU Approach to Data Protection and Privacy

The EU has taken a holistic approach to data protection and views the protection of personal data as a fundamental right to protecting the right to privacy. The EU's GDPR is both a privacy and data protection regulation as organizations must ensure that data is managed and secured, utilizing such tools as encryption software. In addition, they must consider privacy rules and data privacy regulations that allow users to share what they want. The end goal of the GDPR culminates to ensuring transparency between the users and the organization and companies as a means through clear communication and information notices.[60]

The General Data Protection Regulation was designed to synchronize EU member states and their data protection regulations to protect and ensure the personal data of persons residing in the EU. The extra-territorial scope of the European Union GDPR means it applies to any "controller" and "processor" who interacts with EU data subject's personal information inside and outside of its borders.[61] According to Article 3 of the General Data Protection Regulation, the legislation applies to all organizations and companies if they offer free or paid goods and services to EU residents. Additionally, companies and organizations that monitor the behavior of the Eu residents inside the EU or outside the EU must comply with the legislation.

[59]Kai Alderson, "Making Sense of State Socialization." Review of International Studies 27, no. 3 (2001). Accessed June 18, 2021. http://www.jstor.org/stable/20097743, 415.
[60]Michelle Goddard, "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact." International Journal of Market Research 59, no. 6 (2017): 704.
[61]The GDPR defines controller and processor as two different entities. The data controller is a company, or business who determines the "why" and "how" the personal data of data subjects from the EU should be processed. The processor is usually a third party to whom the controller may sell or give personal data. Therefore, the processor company or entity must also abide under the GDPR. If a company is both, then they are a "join controller."

In order for multinational organizations or companies to collect and use EU residents' personal data, they must comply with the regulations. The GDPR website further details that collecting email addresses from family and friends to create a fundraise or business project can make someone applicable under the data protection and privacy regulation; however, simply collecting the email addresses of friends and family for a picnic[62] Simply put, the people and companies engaging in "professional, or commercial activity" are subject to the law.[63] Only small companies with less than 250 employees are exempt to some degree, such as not being obligated to record-keeping of their activities.

Rights and obligations of users and obligators

Of the most critical aspects of the GDPR, service providers have extensive obligations and outlined rights guaranteed to data subjects, a person whose data is collected. Based of seven principles, the rights are outlined in Chapter three from Article 12 to 23, while the obligations can be read in chapter four from Article 23 to 43. These rights are impactful because they give users more control over the utilization of their personal data. The eight rights can be summarized as:

1. The Right to Information
2. The Right of Access
3. The Right to Rectification
4. The Right to Erasure
5. The Right to Restriction of Processing
6. The Right to Data Portability

[62] "Does the GDPR Apply to Companies outside of the EU?" GDPR.eu. February 13, 2019. Accessed June 08, 2021. https://gdpr.eu/companies-outside-of-europe/.
[63]Ibid.

7. The Right to Object
8. The Right to Avoid Automated Decision-Making

Essentially, the rights are designed so that users are aware of what is happening to their personal data. On the other hand, the obligations of the controller of any entity that processes data are meant to ensure compliance. The right to ratification for example, enables users to request controllers to update incorrect information that the businesses have about the data subjects. Even further, a data subject can request that the personal data collected be deleted. This is also called the "right to be forgotten."[64] Data subjects also have the right to know where the information came from and how long their information will be held. This means that companies are obligated to make sure information is presented so that data subjects can understand how their data is being collected and what kinds of data it is. Companies are also obligated to ensure that the request for information is responded to is fulfilled within one month or inform data subjects of an extension. Additionally, businesses should inform data subjects about their personal data even if they were not the information collector. If companies have access and are doing anything with that data, users must be informed about it as well.

The purpose of collecting personal data must have also been defined initially at the time of collection, which means that the repurposing of personal data is not allowed under the GDPR. Instead, if the data subject feels like the original purpose of the personal data already collected may have changed without their consent and illegal, they can request that their data be removed. If a company re-uses personal data for a new purpose, they cannot do so without notifying and first getting consent from the data subjects.

[64] Ibid.

Controllers should seek consent from data subjects before deciding to share their information with another company. This consent could have been obtained originally at the first collection or at a later time. However, data subjects must have permitted their personal information to be transferred by "automated means."[65] The GDPR does, however, allow retention of personal information if the purpose pertains to "archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1)."[66] The GDPR also recognizes that the use of A.I. and supercomputers may lead to profiling and other automated decision which may affect data subjects negatively. Data subjects can object to their data being it is not authorized by the Union or member state for legitimate reasons such as national security. If the data subject consents to their data being used for the automated decision, then their data will continue to be used in such a manner.

Adequacy Requirements

Another critical aspect of the GDPR is the adequacy requirements. Adopted from the EU Directive, the adequacy requirement states that for personal data to transfer to or from a company or organization outside the EU, the European Commission is given the power as stated in article 42(2) of the GDPR, to determine if that company meets or country offers an equivalent level of data protection to the EU. Once the commission has proposed, the European Protection Board forms an opinion, receives approval from the EU member state, and finally adopts a position by the European Commission.

Cross-broader transfer of EU residents' data entails that "third countries" as defined under the GDPR also provide adequate protective safeguards to receive EU residents' personal

[65] "Art. 20 GDPR - Right to Data Portability." GDPR.eu. July 23, 2020. Accessed June 14, 2021. https://gdpr.eu/article-20-right-to-data-portability/.
[66] Regulation, General Data Protection (2016)

information. However, only 12 countries satisfy the general requirements of obtaining a "suitable level of protection based on adequacy decision" by the European Commission, meaning their national privacy laws were akin to EU law.[67] These countries include Andorra, Argentina, Canada (only commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, Japan, and Canada. South Korea is expected to join this list as they have recently completed talks with the commission. According to the European Union Court of Justice, the U.S., for example, has fallen out of compliance with the current Privacy Shield since it was deemed inadequate. In one report in 2019, India was ready to seek "adequate" status with the GDPR. The goal of meeting the adequate demands of the EU is to ensure transnational relationships continue.

Consequences

Lastly, adequate data protection legislation such as the GDPR includes the ability to sue an organization when they have failed to successfully protect against a breach or have used an individual's personal data outside of their intended use. The GDPR allows data subjects to bring to court multiple actors including the controller and the processor if they can prove that the organization has cause them distress or harm.[68] Controllers and processors can be charged up to 10 million Euros for breaking certain articles pertaining to consent and collect of children's personal data or up to 20 million Euros for failing to oblige data subject the rights guaranteed or transferring data to third countries who do not fulfil the proper adequacy ruling.

[67] "Third Countries." General Data Protection Regulation (GDPR). August 13, 2020. Accessed June 19, 2021. https://gdpr-info.eu/issues/third-countries/.

Chapter IV: The United States

The United States data protection regulations have often been described as "patchy." [69] Unlike the EU, there is no omnibus law that governs the limitations and activities of the private sector. Instead, it has historically been sector-specific rulings and legislations. In addition, the U.S. traditionally follows a laissez-faire or hands-off approach regarding the private industry, which means that they have often relied on industries to self-regulate.[70] As described by lawyer Micheal Ryan, the private sector's scope of limitations and activities on the use of personal information have often been in an "ambiguous" state, thus leaving the consumer privacy and the personal data of users at the hands of tech companies who often fail to adopt any adequate data protection regulations.[71]

Privacy in the U.S.

Unlike the EU, where privacy and data protection are codified, in the U.S., the right to privacy is not clearly stated as a constitutional right as much as it has been touched upon in various cases in the 1960s and 1970s. Most often, the right to privacy is alluded to in the Fourth Amendment in the Bill of Rights, which denies the intrusion of anyone on a person and their property. Amendment four states that a person has the right to "be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures," from another, including that of Government or police without a warrant.[72]

In the ruling on *Katz v. the United States* case, the U.S. Supreme Court deemed that the fourth amendment in the Bill of Rights safeguarded "individual privacy," not the "right to

[69] Ibid,7.
[70] Ryan Moshell, "And then there was one: The outlook for a self-regulatory united states amidst a global trend toward comprehensive data protection." Tex. Tech L. Rev. 37 (2004): 374.
[71] Ibid,375.
[72] Fourth Amendment, Bill of Rights

privacy" in cases of "unreasonable searches and seizures without a warrant."[73] The case involved Charles Katz, a bettor wiretapped by the FBI on a public telephone and was later arrested. The decision by the Court in favor of Katz overturned the previous decisions made by the circuit and the district court. The Supreme Court deemed that the FBI did not have a warrant to be tapping public telephones and broadened the scope of the fourth amendment to include activities such as wiretapping or listening to someone's conversation as intruding upon "private discourse."[74]

Other significant cases such *as Carpenter v. the United States, Whalen v. Roe* established and called upon "informational privacy" or information dealing with the "personal matters" and "physical matters" of a person. In *Carpenter v. the United States*, the Supreme Court deemed that the F.B.I. also did not obtain a warrant to retrieve or trace the location of Carpenter, who, along with six other men, conspired to rob a bank. The FBI. used location information collected by cell carriers to trace Carpenter's phone and arrest him. The Court ruled Americans should expect "a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which "hold for many Americans the 'privacies of life" contradicted the actions of the F.B.I.[75] In the case of *Whalen v. Roe*, a group of patients challenged a New York State law requiring patients' personal information such as their name, address, and age to be shared with pharmacies and the state and to be recorded electronically. The patients deemed the sharing and display of their personal information on prescriptions and on the computer to invade their privacy. The Supreme Court agreed in favor of new state law and deemed that collecting personal information was not a violation of the fourth amendment. The collection of personal information posed no immediate threat if the collection would prevent

[73]Stephen P. Mulligan, W. C. Freeman, and C. D. Linebaugh. "Data protection law: an overview." In R45631. Congressional Research Service. https://crsreports. congress. gov/product/pdf. 2019,5.
[74] https://supreme.justia.com/cases/federal/us/389/347/#tab-opinion-1946919
[75] CARPENTER v. the UNITED STATES, 422 U.S. 853 (1975), page 2.

drug abuse, and it was not different from the conventional means of collection and storing information.[76] The new law would not violate "constitutionally protected privacy rights," since it was to be shared with only a small number of people, and there were numerous safeguards that would protect the personal information of patients being stored on the computer.

Overall, earlier cases in the U.S. hinted at the right to informational privacy, and many cases that were brought to court primarily involved the U.S. government. Therefore, many of the currently existing data protection regulations exist to protect American citizens from their government. The idea of information privacy floated in the U.S. Supreme Court, but as congressional research on the *Data Protection Law: An Overview* revealed, the courts never really attempted to claim informational privacy as a right even though lower courts recently look to some degree at people being afforded some type of informational privacy.[77]

History of Sector-based Data Protection Legislation

The most well-known data protection regulation in the U.S. curbed Americas' federal government surveillance tactics on U.S. citizens, a reaction to the Watergate scandal where federal agencies were able to illegally surveil and investigate the political enemies of then-president Richard Nixon and store their personal information.[78] The Privacy Act of 1974 introduced the purpose limitation on the federal agencies who were only to collect necessary information and mandated federal agencies to create procedures to protect this information.[79] Although not worded as a right, the ability for individuals to access and ask to amend their own records maintained by federal agencies was also part of the Privacy Act of 1974. While other

[76] https://supreme.justia.com/cases/federal/us/429/589/#tab-opinion-1951999
[77] Stephen P. Mulligan, W. C. Freeman, and C. D. Linebaugh, "Data protection law: an overview." In R45631. Congressional Research Service. https://crsreports. congress. gov/product/pdf. 2019,10.
[78] Ibid,6.
[79] Ryan Moshell, "And then there was one: The outlook for a self-regulatory united states amidst a global trend toward comprehensive data protection." Tex. Tech L. Rev. 37 (2004): 357.

federal legislation has since been created to address the protection of personal data of a person, they have mainly focused on specific industries, including the financial and healthcare industries.

One crucial financial legislation includes the Gramm-Leach-Bliley Act signed in 1999, which protects consumers' non-public information (NPI), or information not publicly available from being shared with third parties involved in marketing practice. The Act also obligates financial institutions such as banks to give notices to customers on how their NPI was being shared and develop a mechanism that safeguards consumers' information. Thus, the Bill essentially obligated businesses to be transparent, protect consumers' NPI, provide an opt-out option, gives customers the right to access their information, and focuses on ensuring customers' privacy.

HIPAA or the Health Insurance Portability and Accountability Act is another necessary federal regulation that addresses the personal information of patients. This Act protects the health records of patients, also known as "protected health information" (PHI). PHI includes things used to identify a patient, such as their SSI, name, billing information, photos, and health information. All healthcare providers, including hospitals, health insurance companies, and health care clearinghouses, are subject to follow the rules under HIPAA. HIPAA guarantees a set of rights for patients and obligations of companies that must comply with to ensure that PHI is in fact protected when transmitted by electronic means. Patient rights include the right to access one's personal health information in any form, the right to correct their information, the right to be notified about the use of their health information, how it is shared, and the right to opt-in into marketing purposes.

Companies that are liable under HIPAA are also expected to follow The Security Rule, which includes conducting risk assessments that show areas where protected health information

could be at risk to unauthorized access or exposure and fix them. There is a limitation clause on the use of data, safeguard required, and limitations on who can view protected health information. Employees must also be adequately trained to keep patient information safe. Aside from a few other industries based federal data protection regulations, big tech and social media giants such as Facebook, Google, Amazon, Microsoft, etc., have no sector-based or federal law that they must abide by.

Use of Fair Information Principles and the FTC

Another vital practice by the U.S. has been using the fair information practices mentioned earlier, which has guided the U.S. approach on federal laws on the use and collection of personal data. It was utilized in the Privacy Act of 1974, employed in the other U.S. federal privacy laws, but failed to bring about any changes. According to Fred H. Cate, Director at the Center for Applied Cybersecurity Research, the use of the FIPPS framework in "delivering a high standard of effective, predictable, and efficient data protection, or meaningful consistency among nations or regions" have not gone far enough or often lack a more robust mechanism that truly protects privacy.[80] Since 1974, the Federal Trade Commission has promoted a series of fair information practices principles (FIPPS) for businesses to adopt to provide information privacy for consumers. These FIPPS were reported in a 1999 report to Congress after the Federal Trade Commission examined the privacy concerns of consumers using the internet to purchase products. [81] In the 2000s, the FTC report was considerably "watered down" from the previous.[82]

For the FTC, businesses are encouraged to adopt regulatory practices on personal information online by ensuring that consumers are aware of a company's business practices about

[80]Fred H Cate, "The failure of fair information practice principles." Consumer protection in the age of the information economy (2006), 369.
[81]Robert Gellman, "Fair information practices: A basic history." Available at SSRN 2415020 (2017), 352.
[82]Ibid, 365.

collecting information; consumers have the option to consent to how their data will be used. In addition, consumers can either opt-in to have their information collected or opt-out, which suggests that consumers must be aware of that and must act on their end to stop any information from being collected or shared.[83] Additionally, the principles also included free access for consumers to view the information collected about themselves, for this information to remain accurate and up to date, for the data to be secured, and not be at risk of exposure and access from outside or unauthorized access. Companies are also encouraged to use encryption measures and maintain secure servers to keep consumers' information from being accessed by unauthorized personnel. Lastly, the principle of enforcement/redress advocates for businesses to decide to self-regulate themselves or have an enforcement mechanism to ensure that the other principles are being protected.[84] The FIPPS are as followed: Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security and Enforcement/Redress. In the 2000s report, Enforcement and Redress were erased from their report to Congress.[85]

Since the mid-2000s, other U.S. agencies have also come forward with their versions of FIPPS driven by a lack of coherence. In 2015, the Obama administration also published proposed draft legislation of an omnibus data protection regulation called the Consumer Privacy Bill of Rights Act. It also aimed to give the Federal Trade Commission the power to enable it to wield more power now that codes of conduct or principles were codified into law, and companies would have to ensure adherence. The Act would also position consumer privacy as a right and warrant companies to ensure their right was upheld. In this draft, the administration adopted a more international standard of FIPPS like the OECD than the FTC.[86]

[83] Ibid 352.
[84] Ibid, 351.
[85] Ibid, 352.
[86] Robert Gellman, 39.

Issues and failures with privacy and data protection in the U.S.

Overwhelmingly, Americans have issues in entrusting their personal data to the private and public sectors. According to a Pew Research published in November 2019, 62% of Americans expect their data to be collected by companies daily, and 63% expect their information to be collected by the government. Overall, Americans feel that they are being surveilled whether they are online or offline.[87] Due to the lack of comprehensive data regulation, weak internal mechanism, lack of accountability, the U.S. has often been the source of significant data breaches. In addition, the U.S. government has also been in hot water due to its surveillance practices abroad and at home.

In the previous case mentioned at the beginning of this paper, companies like Yahoo are unwilling to admit to data breaches. Americans do not expect companies to confess if they have used the information collected as they initially intended to use it, as 80% of respondents already believed it was happening. Even with the already existing federal sector-based legislation focused primarily on the business and medical/healthcare industries, these sectors are also more prone to data breaches.[88] In 2019 and 2020 alone, the number of medical records exposed remained relatively high at about 155 to 165 million. Furthermore, at least 64% of adults in American have been impacted or experienced a data leak of their personal information.[89]

The Pew Research in 2019 strongly suggest that Americans currently do not feel that their personal data is secure as 70% of Americans reported that they felt that compared to 5 years

[87] ibid
[88]Council of Economic Advisers (U.S.). 2018. The cost of the malicious cyber activity to the U.S. economy. https://purl.fdlp.gov/GPO/gpo89296.
[89] Aaron Smith, "Americans and Cybersecurity." Pew Research Center: Internet, Science & Tech. August 17, 2020. Accessed June 18, 2021. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/.

ago, their data was less protected. Consumers and other governments are wary of U.S. products due to the reach of surveillance powers.[90] AI technology has also given the U.S. the advantage to become the world leader in the tech industry. Companies like Facebook, Instagram, and Twitter sell consumer data for about 44 billion a year.[91] The fallout of the Edward Snowden leaks in 2015 also revealed that the National Security Agency (NSA) had an extensive spy program. They were tapping into U.S. companies like Google and Facebook and tracking users' communication, tapping into fiber- optic cables in Europe, listening in on phone calls, and collecting internet traffic.[92] In addition, they bugged the offices and embassies of their closest allies.

According to researchers Nuala O'Connor, Althea Lange, and Ali Lange, this increases surveillance from the federal Government poses a risk for the loss of revenue to the private sector. Businesses have difficulty convincing their overseas consumers and the Government that their data is protected from U.S. government surveillance. As the companies that also store the most personal information also come from the United States, the fallout from the Edward Snowden report led tech companies to report that the tech industry could lose up to 25% of revenue or 180 billion dollars from lost customers.[93]

Data protection legislation has often been in reaction to government overreach and to protect civilians' personal information from being collected by the U.S. government. In contrast,

[90]Claire Cain Miller, "Revelations of NSA Spying Cost U.S. Tech Companies." The New York Times. March 21, 2014. Accessed June 18, 2021. https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.
[91]Kari Paul, "Americans' Data Is Worth Billions - and You Soon Might Be Able to Get a Cut of It." MarketWatch. October 09, 2018. Accessed June 19, 2021. https://www.marketwatch.com/story/americans-data-is-worth-billions-and-you-soon-might-be-able-to-get-a-cut-of-it-2018-10-09.
[92]Claire Cain Mille, "Revelations of NSA Spying Cost U.S. Tech Companies."
[93]Ibid.

the private sector has been left to regulate itself, create data protection regulations they see fit or adjust in reaction to regulations such as the General Data Protection Regulations from the E.U.

An increasing consensus among Americans is that the Government needs to intervene in the use of personal data by companies, as 75% felt that they had no confidence or little confidence in the companies being held accountable if they were to misuse their data. The efforts by the White House and even other agencies releasing new FIPPs have shown government agencies' effort to engage on the issue but there is an absence of coherence across government agencies.

The current federal sector-based laws that require infrastructure to protect patients' information in the health care industry and the financial industry have also failed to protect against data breaches. According to the U.S. Department of Health and Human Services website, which reports data breaches that affect more than 500 people, 642 data breaches were reported in 2020 alone. Hacking and I.T. incidents accounted for 67% of the breaches, but 92% of the records were healthcare data.[94] In 2019, according to a ProPublica report, patient medical images stored using Picture Archiving Communication Systems (PACS) servers were not only being exposed but also left unsecured by improper safeguards. The system used by multitudes of U.S. healthcare also exposed patient data protected under HIPAA.[95] In June 2021, the Human and Health Services Office of Information Security: Health Sector Cybersecurity Coordination Center (HC3) issued a sector alert for healthcare organizations to review their PACS servers as the issue remained two years down the line. According to the sector alert, the PACS server system, which stores medical images using the Digital and Communications in Medicine Format

[94]"2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020." HIPAA Journal. March 03, 2021. Accessed July 10, 2021. https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/.
[95]Marco, Eichelberg Klaus Kleber, and Marc Kämmerer. "Cybersecurity challenges for pacs and medical imaging." Academic Radiology 27, no. 8 (2020): 1127.

(DICOM), exposed 2 million patients protected health information along with 275 million medical images.[96] The alert also pointed out that healthcare organizations failed to respond to the [first] report in 2019, and the latest report found that they had not heeded the warnings by addressing the vulnerabilities of the PAC's servers, which includes performing ongoing risk assessments and securing open ports, which hackers have been able to exploit. "There's no magic in it. Use the free tools available, and if an organization sees their enterprise listed, then they will know something is wrong."[97]

Since no independent agency protects consumers' personal data, the FTC has often been dubbed the protector of consumer rights. In a 2000s report, the Federal Trade Commission acknowledged that enforcement was failing and that some companies were simply not adopting proper safeguards. The FTC lacks monitoring abilities mainly because of the absence of power defined in the FTC ACT, limiting how much the FTC can regulate the private sector.[98] The Federal Trade Commission is a small organization, where only 50 staff members are focused on privacy among the 1,100-agency staff.[99] The agency's scope of power also does not allow it to push companies to adhere to fair business practices. Since businesses outside of the federal sector-based laws self-regulate themselves with the data policies, they can only be caught conducting unfair practices once they have put out a policy and have not adhered to it.[100] According to a New York Times article, the void of an independent agency on data protection

[96] United States. Dept. of Health and Human Services. HC3: Sector Alert. *Picture Archiving Communication Systems (PACS) Vulnerabilities*. Report: 202106291300. HHS Office of Information Security: Health Sector Cybersecurity Coordination Center (HC3), June 29, 2021.Accessed July 10, 2021.https://www.hhs.gov/sites/default/files/pacs-vulnerabilities.pdf
[97] Ibid.
[98] Chris Jay Hoofnagle, Woodrow Hartzog, and Daniel J. Solove, "The FTC Can Rise to the Privacy Challenge, but Not without Help from Congress." Brookings. August 08, 2019. Accessed June 13, 2021. https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/.
[99] Ibid.
[100] Ibid

has “left Americans at the mercy of digital services that have every reason to exploit our personal information and little incentive to safeguard it.”[101] According to Brooking's report, the agency also closed its door twice in the 1980s, forced by Congress when they deemed the agency to be too aggressive in its practices.[102]

Many of the big tech giants such as Amazon, Google, Facebook, Microsoft have mostly gone unchallenged for their vast collection and use of the personal data from consumers and users who use their applications. A few significant data breaches have resulted in large civil suits and litigations from significant companies. Cases such as these have only increased in the last few years, but not every state has a data breach statute. Although most do, it only includes a notification to consumers. Many do not include a right of action, which allows consumers to sue and bring a company to court for the exposure of their personal data.

In the U.S., privacy and data protection faces an obstacle in the public sector as well. In a 2019 report from Freedom House, internet freedom declined in the United States for the third straight year due to the federal government's mass surveillance.[103] In what can be described as a fight against terrorism and maintaining national security, U.S. agencies like the Department of Homeland Security (DHS) and other law enforcement have" expanded their surveillance of the public, eschewing oversight, transparency, and accountability mechanisms that might restrain their actions."[104] Personal information, social media records, and phone conversation are being stored in databases by the Government and used to analyze individuals that can make inferences.

---

[101]Natasha Singer, "The Government Protects Our Food and Cars. Why Not Our Data?" The New York Times. July 02, 2019. Accessed November 14, 2021. https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html.
[102] Ibid.
[103] Freedom House, "Freedom on the net 2019: the crisis of social media." Freedom House.November 4, 2019.Accessed June 11, 2021,6. https://freedomhouse.org/sites/default/files/2019-11/11042019_Report_FH_FOTN_2019_final_Public_Download.pdf
[104] Ibid, 22.

While many Americans are aware of the monitoring of their online and offline activities, the trade-off between security and privacy remains a big issue. In 2016, 56 % of Americans believed the U.S. was not going far enough to protect the country, while only 28 felt that the Government had gone too far and restricted civil liberties. Just before that, in 2014, right after the report from Edward Snowden, 53 % disapproved of the Government's collection of telephone and internet data. In 2019, 64 % expressed concerns over how the Government uses the data collected. The U.S. is often in limbo, trying to navigate civil liberties while trying to secure the borders. The latter has often been deemed more urgent and vital, thus leaving privacy for later.

Interest groups have long played an essential role in U.S. politics by lobbying local, state, and federal politicians to cater to their needs. These groups can influence legislation by lobbying politicians or indirectly lobbying to influence the public's views. The other way groups gain influence is by giving money in campaigns to make decision-making outcomes more favorable. While Apple CEO, Tim Cook and other big tech companies have lauded the GDPR and have called for a comprehensive data protection regulation in the U.S., they still, according to a report by National Public Radio (NPR), hope that by pushing state legislation, including helping to write them, they will be able to sculpt legislation to their advantage and weaken it. The report also suggested that Big Tech is getting involved directly with sponsoring and writing bills. For example, Virginia's Bill, which was initially authored by Amazon and Microsoft, and which passed, is much weaker compared to CCPA and sees companies trying to push for 14 other state bills like this. Ultimately the goal they say is to override the CCPA by pushing for the much weaker federal initiative. In the case of Connecticut lobby groups, the Bill introduced by Connecticut Senate Majority Leader Bob Duff ended failing due to what he recalls as lobbying efforts of big tech groups.

Adoption of data protection regulation since the EU GDPR

Individual states in the U.S. have shown that they can adopt similar data protection regulations like the GDPR. State-created consumer privacy legislation also shows signals constituents' feelings about their privacy and data protection from a state level. As more states adopt similar legislation which prevents cross-state data transfers in the country unless adequate data protection exists in that other state, the federal government will eventually be faced with a choice to address this issue as more abuses from the private sector on consumer data arises. However, state legislation also adds to the list of countless and recent adoptions of data protection regulations that already exist in the U.S.[105]

While the federal government has failed to implement comprehensive data and privacy legislation, state legislation on data protection has multiplied in the past three years on the heel of the GDPR. On January 1, 2018, California passed the California Consumer Privacy Act (CCPA). Notably, Silicon Valley holds some of the biggest tech agencies like Google and Facebook, which benefit from cross-border transfer with the EU. The CCPA has been hailed as a steppingstone to adopting an adequate federal data protection regulation in the US. It has also inspired other states across the U.S. to jump on board. It is evident that the Bill takes some of the inspiration from the GDPR. Some of the rights under the California Consumer Act include the right of a consumer to know how their information is being used for, the right to ask businesses to disclose what information they have collected, and what information will be shared with third parties. The Bill also gives Californians the right to be forgotten, the right to be deleted from databases, the option to opt-out of data sharing, and non-discrimination if consumers decide to utilize their rights under the CCPA. In total, the CCPA introduced a series of five rights that

[105] Nuala O'Connor, "Reforming the U.S. Approach to Data Protection and Privacy." Council on Foreign Relations. January 30, 2018. Accessed June 16, 2021. https://www.cfr.org/report/reforming-us-approach-data-protection.

consumers are entitled to. They include the right to know(access), right to notice, right to opt-out, anti-discrimination, and the right to deletion(erasure).

Three other states have enacted a comprehensive data protection law, including Nevada, Virginia, and Colorado. Nevada had an existing law, but its new legislation aims to add to the existing one to prevent consumer personal information from being sold if consumers opt-out.[106] In other states, seven legislations are currently "in committee," meaning that while these bills have been sponsored, they are currently going through public hearings. This process is used to see the current viewpoints on the issue, going through "mark-ups," which means amendments may be made.[107] The committee then makes various decisions, such a tabling the Bill or moving forward with the Bill, which means it goes on to a vote.[108] Colorado's legislation was only passed on June 8th. Currently, there is no set a date for the signing of the Colorado bill, but it will not be enforced until the governor has signed it.

According to the National Conference on State Legislature in 2019, 24 states have introduced Consumer Data Privacy legislation.[109] The consumer data privacy legislation is not comprehensive nationally; however, comprehensive privacy legislation saw the most significant number of bills introduced at a state level. The NCSL outlines that their list only includes states who introduced "regulation of privacy practices of commercial entities, online services or commercial websites, covering legislation related to the privacy of consumer data, including bills

[106] Ibid.
[107] In Committee. Accessed June 14, 2021. https://www.house.gov/the-house-explained/the-legislative-process/in-committee.
[108] Ibid.
[109] Pam Greenberg, Lesley Kennedy. 2019 Consumer Data Privacy Legislation. January 3, 2020. Accessed June 14, 2021. https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

related to online privacy, collection of consumers' biometric data, data broker regulation and other miscellaneous consumer privacy issues."[110] In 2020, that number was up to 30.[111]

[110] Pam Greenberg, 2020 Consumer Data Privacy Legislation. January 17, 2021. Accessed June 14, 2021. https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx.
[111] Ibid.

Chapter V: India

India is relatively new to data protection and privacy legislation regime and, like the U.S., only has specific legislation for sectors. India is also a BRIC country, joining Brazil, Russia, and China, which are seen as emerging economic powerhouses, currently dominating the goods and services industry. Last year, they also became the fifth largest economy, jumping from eighth place in just ten years and overtaking France and the United Kingdom. India also comprises the second-largest population behind China, with 1.6 billion people, and is the largest democracy. Also noteworthy is that the EU is also India's third-biggest trading partner, just behind the U.S. and China. As an emerging country, Indians are also increasingly using the world wide web and accessing social media platforms, shopping, or buying more smartphones. According to the World Bank, internet penetration in India was 41% in 2019, meaning that under half of the population has access to the internet.[112] Ten years ago, this was only seven percent. About 50% of the Indian population has access to a social media account in terms of social media. India's economic growth is mainly powered by domestic demand, but foreign trade is critical as India's increasing role in the international community. This means that it must also address new issues rising in its own borders and adapt to the growing consensus for data protection in the international community. To be left behind may severely impact India's growth. The questions of privacy and data protection have caught up to India as it has become one of the "world's largest destinations for the international outsourcing of processing of personal information ('business process outsourcing')." [113]

---

[112] The World Bank, International Telecommunication Union (ITU) World Telecommunication/I.C.T. Indicators Database. Individuals using the internet (% of the population). Retrieved from https://data.worldbank.org/indicator/IT.NET.USER.ZS

[113] Graham Greenleaf, "Promises and illusions of data protection in Indian law." International Data Privacy Law 1, no. 1 (2011): 47.

Privacy in India

Like the United States, the right to privacy in India has been contested in court, but it was finally codified into their constitution in 2017. When India became independent from Britain in 1947, there were calls to establish the right to privacy in its constitution. However, it failed as many thought it would pose a problem for the investigations and powers of the states if the right to privacy meant "it would elevate every private/ civil communication to that of State papers."[114] Attempts on including the right to privacy were made by making similarities to the U.S. fourth amendment and the German and Irish constitutions.[115]

Articles 19 and 21 were inferred to guarantee some rights to privacy as determined by the Supreme Court in various cases. Article 19 dealt with providing freedom of "speech and expression …without the fear through oral/written/electronic/broadcasting/press," implying that one has the right to say or express and broadcast without fear of persecution. Article 21 secured two rights, the right to liberty and the right to life, essentially preventing the state from infringement upon one right to liberty without due process and according to the laws of the land first. However, both articles did not suffice in one of the earliest cases where defendants argued that their right to privacy was at risk.

In 1954, in the case of *M.P. Sharma & Ors. vs. Satish Chandra and Ors*, the Indian Supreme Court ruled that the right to privacy was not in the constitution and that the original authors of India's constitution did not see it fit to have such a right which they compared to the U.S. Fourth Amendment. The case dealt with the right to property, a right which was removed from India's constitution in 1978, and the right to which the Government had to "search and

[114] Sargam Thapa. " The Evolution of Right to Privacy in India International Journal of Humanities and Social Science Invention (IJHSSI). February 2021. Accessed June 16, 2021. https://www.cfr.org/report/reforming-us-approach-data-protection, 54.
[115] Ibid,55.

seizure" documents on the defendants' property. The defendant claimed that their right against self-incrimination, as stated in article 20 and the right to privacy, had been violated as the searches had self-incriminating documents. The Court deemed that the state was above and within its own power to do so and take away the items and that such activities were only temporary and did not infringe upon their property right completely.

Another earlier case that presented the right to privacy in terms of surveillance was the *Kharak Sigh v The State of UP* in 1962, which involved the defendant, Kharak Sigh, who had been released from jail due to a lack of evidence after being accused of bank robbery. The police department that had arrested him started surveilling the defendant, creating a so-called 'History Sheet' which enables the police department to track his movements.[116] The department also had visits to the defendants' home at odd hours throughout the day and night and which Kharak claimed was in violation of his right to privacy which was constituted in the right to life and liberty in Article 21 of the constitution. Like the earlier case, the Court ruled that the right to privacy was irrelevant since it was not a right guaranteed in the Indian Constitution. Kharak's right to life and liberty was hindered by the police who came to the defendant's home. The police department provisions were deemed unconstitutional and restricted Kharak's right to life and his right to movement as directed in Article 19.

In the two mentioned cases, the right to privacy was brought up by the defendants but was struck down by the Supreme Court, which denied that the right to privacy itself existed in the constitution, so it was not applicable for the defendants to use in Court. However, at the end of the Kharak case, one of the justices, Subba Rao, acknowledged that privacy was a facet of liberty.[117] In the cases following 1975, the Court determined that to some degree of the right to

[116] Ibid.
[117] Ibid.

privacy did exist but that it would almost follow a common law approach in which courts decide on a case-by-case basis from previous cases since there is no official written or codified law that applies. It was not until the case involving Justice K.S. Puttuwamy which brought about a change and a decision by the 9 Supreme Court justices to add the right to privacy in Part III of the India Constitution.

Regarding judicial recognition of the right to privacy, in 2017, the Supreme Court of India declared that privacy was a fundamental right, even acknowledging that privacy was endangered with the rise of technological advancements. In the court case of *Justice K.S. Puttaswamy (Retd) vs. Union of Indi*a, the Court upheld that article 21 of the Indian Constitution by saying that "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution." [118]

Data Protection Legislation

In India, preexisting legislation on data protection has often concentrated on the communication sector, and the issue with this legislation is that they have often lack oversight. Aside from the communication sector, the other existing legislation aimed at protecting the stored information on citizens is about India's biometric system created in 2009.

The Information Technology Act, 2000 (IT Act) was the beginning of India's move towards something resembling that of a data protection law. The original act had been modified on multiple occasions in 2008 and 2011. The Act addressed the growth of "electronic commerce," or the buying or selling of products online, and sought to punish those who misused

[118] Panday, Jyoti. "India's Supreme Court Upholds Right to Privacy as a Fundamental Right-and It's About Time." Electronic Frontier Foundation. October 11, 2017. Accessed June 19, 2021. https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time.

consumers' data and prevent theft and other cybercrimes.[119] The act only punished individuals who hacked the system rather than the organization that held the data. The 2008 amendment added sections 72A and 43A security practices and procedures to prevent sensitive personal data or information from being disclosed. If an individual's sensitive personal data was found to have been compromised, individuals were liable to sue the companies.[120] In 2011, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules were imposed, which required additional prerequisites on businesses in India dealing with the collection and disclosure of sensitive personal data or information.

In 2016, The Aadhar Act, as determined by the Supreme Court, legitimatized the use of Aadhaar, the controversial biometric identity program that assigns each Indian resident a 12-digit number. Aadhaar shares similarity to the Social Security Number system in the U.S., where everyone is assigned a number that can be used to carry out official business. Aadhaar is voluntary and was initially intended to receive welfare benefits but is used for other things such as opening accounts and registering for school. Information collected by the Unique Identification Authority of India (UIDAI), which oversees Aadhaar, is deemed sensitive personal information needs to be protected against unauthorized access and follows the provisions outlined in the IT Act.

Comprehensive Data Protection legislation

In 2019, the Personal Data Protection Bill (PDP) was proposed to create India's comprehensive data protection law. The Bill is currently still in its first stage. For a bill to become a law in India, a bill must go through three stages that include "introduction,

[119] Yogesh Kolekar, "A Review of Information Technology Act, 2000." Available at SSRN 2611827 (2015),1.
[120] Ibid.7.

consideration, final passage, and must also be given presidential assent."[121] India being a parliamentary system modeled after the UK means that a bill must go through the legislative branch, which consists of the Parliament, including the lower house, the upper house, and then the president. The first stage includes introducing the Bill while also having a Standing Committee examine concerns and then reports on the Bill. If the Bill passes the first stage, the second stage is the consideration phase, which comprises two parts. The first part of this stage is the discussion on the Bill in the house, and they may opt to consider it right away or send it off to a committee again who will look at the Bill on a clause-by-clause basis or welcome public opinion on the bill Amendments.

The second stage includes a clause-by-clause analysis done and amendments are made and voted on. The third stage includes making additional amendments only allowed through specific means, and a simple majority vote is necessary to get the Bill passed.[122]Additionally, if the PDP amends the Indian constitution in any way, over two-third, are required in each house level for it to move forward. Once that is completed, the Bill is sent to the president, who may make recommendations and send back the Bill or sign it into law. The Parliamentary Joint Select Committee has been charged with the first stage but has asked for several extensions so far on deliberations about the Bill since December 2019.[123] It was expected to be submitted in a Budget session earlier this year in January but has been delayed and is expected to be given to the speaker of the house ahead of the winter session of the Parliament.[124]

[121] Tariq Ahmad, National Parliaments: India. February 01, 2017. Accessed June 16, 2021. https://www.loc.gov/law/help/national-parliaments/india.php#Structure.
[122] Ibid.
[123] AM Jigeesh,. "Data Protection Bill: Panel Likely to Finalise Report on Oct 21." Businessline. October 20, 2021. Accessed November 10, 2021. https://www.thehindubusinessline.com/news/national/panel-likely-to-finalise-report-today/article37096906.ece.
[124]Ibid.

Like the GDPR, the Indian Bill will establish a Data Protection Authority of India (DPAI), and companies outside of India are susceptible to the law if they collect or process the personal data of Indians and non-Indians living within their borders. The Bill further identifies particular types of data called "sensitive personal data," which includes health data, financial data, and "critical personal data," which the state will later determine.[125] In addition, the Bill includes the following rights of the data principles or the owner of the data; the right to confirmation and access (Article 17), data portability (Article 19), right to correction and erasure (Article 18), and the right to be forgotten (Article 20).[126] This means that out of the eight rights guaranteed to data subjects in the GDPR, the PDP has five out of the eight rights. Unlike the GDRP, where the data subject has a right to restrict processing when companies or organizations are believed to be outside of the original purpose or deemed unlawful, this right is not explicitly stated in the PDP is not mentioned. Additionally, the right to object is not included in the current PDP bill and is not the same as the right to erasure but an alternative.[127] The right to erasure or right to be forgotten or article 12 means the controller can no longer process information of a data subject, and the right to object is article 21 entails that data was already processed and stopped at a particular stage.[128] Lastly, the rights concerning automated decision-making and profiling are not established in the PDP Bill.

The Bill also includes a section on the obligations that controllers, referred to as data fiduciaries in this Bill and data processors, must fulfill while processing users' data. Some that correspond to the GDPR include data breach notification to both the user and the data authority,

[125] Govind Ram Singh and Ruj Sushmita, "A Technical Look at The Indian Personal Data Protection Bill." arXiv preprint arXiv:2005.13812 (2020), 8.
[126] Gupta Chetan and Lothar Determann,. "India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018." Berkeley J. Int'l L. 37 (2019),16.
[127] Aditi Chaturvedi, "GDPR and India: A Comparative Analysis." Centre for Internet & Society. October 17, 2017. Accessed November 30, 2021. https://cis-india.org/internet-governance/blog/gdpr-and-india-a-comparative-analysis.
[128] Ibid.

storing and recording how personal data is collected and whom it is sent to if they are transferring the data. Other requirements include appointing a data protection officer, an opt-in requirement, and age verification to ensure the personal data of children are not collected and that parents have consented to their children's data being collected data and impact assessment, designed to check systems and protections in place.

The failure to comply with the legislation could set businesses up to 2.1 million dollars of 4% of the annual turnover and an additional 50 million dollars if companies and organizations do accountability checks.[129] Additionally, under the PDP, personally identifiable information and sensitive information are two different things meaning that companies and organizations may not transfer sensitive information across borders, a concern for big tech companies.

Issues with Privacy and Data Protection in India

In 2018, the most significant data breach occurred in India. The breach of the central ID system, also known as the Targeted Delivery of Financial and Other Subsidies, Benefits, and Services, affected almost 1.1 billion records. This also led to India being placed second behind the U.S. on the number of compromised data records in history.[130] Further complicating the issue has been that the Unique Identification Authority of India (UIDAI), who is in charge of the Aadhaar system and has denied any breach ever occurring.[131] Similar to the United States, there is a lack of data protection regulation that exists in the private sector and the issue of national security. Unlike the US, there is a large gap of established data protection regulation on the public sector and government agencies' collection of personal data.

---

[129] Kapil Kajal, "India's Tech Industry up in Arms over Proposed Data Privacy Law." Nikkei Asia. January 10, 2020. Accessed June 20, 2021. https://asia.nikkei.com/Business/Business-trends/India-s-tech-industry-up-in-arms-over-proposed-data-privacy-law.

[130] Joseph Johnson, "Biggest Online Data Breaches Worldwide 2021." Statista. May 25, 2021. Accessed June 16, 2021. https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/.

[131] Prakhar Misra, "Lessons from Aadhaar: Analog aspects of digital governance shouldn't be overlooked." Pathways for Prosperity Commission Background Paper Series 19 (2019),16.

WhatsApp has also recently sued the Indian Government in June 2021 in an attempt by the government trying to surveillance messages, the content of users, and track users' location.[132] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, which is set to replace Information Technology (Intermediaries Guidelines) Rules, 2011 will allow the Government to remove encryption if they deem what is placed on the platform as "misinformation," or if it criticizes the Government.[133]

Since the 2008 Mumbai attack, terrorist attacks on Indian soil have led to a rise of the surveillance industry in India in the name of national security. Some of the largest foreign surveillance tech companies like China's ZTE, Japan's NEC, the US's Verint Systems have found success in the Indian market.[134] Indian companies also contribute to this, such as ClairTrail Technologies, known for their networks that can access and detect networks such as Gmail, Yahoo, and voice calls. These monitoring solutions are often sold to law enforcement.[135]

In 2020, the Delhi High Court issued a notice that would stop collecting the Indian Government from collecting data through their three central surveillance systems. These systems have also contributed to the radicalization of surveillance of Indian citizens, and they are the National Intelligence Grid (NATGRID), Central Monitoring System (CMS), and Network Traffic Analysis (NETRA).[136] The National Intelligence Grid is a highly integrated database meaning it houses multiple databases into one location that came into existence after the 2008 Mumbai attacks and can intercept text messages, phone calls, and social media posts directly

[132] Joseph Menn, "WhatsApp Sues Indian Government over New Privacy Rules - Sources." Reuters. May 26, 2021. Accessed June 20, 2021. https://www.reuters.com/world/india/exclusive-whatsapp-sues-india-govt-says-new-media-rules-mean-end-privacy-sources-2021-05-26/
[133] Ibid.
[134] Sangeeta Mahapatra,"Digital Surveillance and the Threat to Civil Liberties in India." German Institute of Global and Area Studies (GIGA), 2021. http://www.jstor.org/stable/resrep31794,6.
[135] Ibid.
[136] Ibid,4.

without the telecommunication companies providing access.[137] The Central Monitoring System (C.M.S.) project was approved in 2011 and is owned by the Indian Government. It was designed to intercept service providers and record the telecommunication transactions of an individual's call, such as how long it lasted, phone numbers, and the time and date of the call.[138] The Netra system or Network Traffic Analysis uses AI technology to track website traffic, blogs, emails, and Facebook. It was also designed to issue an alert if users search keywords that may potentially place them on a list.

If the PDP is successful in Parliament and passes, one concern highlighted in the Bill is an exemption which provides that the Government does not have to adhere to this legislation. Since the PDP is an all-encompassing law governing both the private and public sectors, the Government can collect and process the information of data subjects under the claim of national security.[139] Critics worry that the Government may use the information for tracking and surveilling civilians and, more so, lead to corruption. The other concern is the adoption and implementation of the Bill, which is seen as burdensome to many small business owners in India. While big tech Giants like Facebook and Google are willing to adhere to the Bill, most of India's businesses are still growing.[140]

[137] Prabhjote Gill, "India's Three Main Surveillance Projects NATGRID, C.M.S. and NETRA Have Been Directed to Stop Collecting Data Citing Breach of Privacy." Business Insider. December 02, 2020. Accessed June 20, 2021. https://www.businessinsider.in/tech/news/indias-three-main-surveillance-projects-natgrid-cms-and-netra-have-been-directed-to-stop-collecting-data-citing-breach-of-privacy/articleshow/79529256.cms.
[138] Ibid.
[139]Manasi Gopalakrishman, "India's Personal Data Privacy Law Triggers Surveillance Fears: D.W.: 11.11.2020." DW.COM. 2020. Accessed June 20, 2021. https://www.dw.com/en/indias-personal-data-privacy-law-triggers-surveillance-fears/a-55564949.
[140] Ibid.

Chapter VI: Discussion, Recommendations, and Conclusion

California has made massive improvements to its first Bill, as seen with the introduction of Proposition 24, which voters approved in the November 2020 election. With over 56% of Californians voting to add the right to accuracy, data portability and built upon the right to opt-out, including consumers who have the right to opt-out of businesses' using "automated decision-making technology."[141] Proposition 24 has introduced an enforcing board called the California Privacy Protection Agency to ensure that companies and organizations will comply with the standards outlined in the CCPA. Like the CCPA, businesses are expected to face penalties from 2,500 to 7, 500 if they do not comply with the Bill.

When the CCPA goes into effect in 2023, it will be the most advanced consumer privacy law in the US, put up against the GDPR. One critical divergence between the GDPR and the CCPA is the right to object vs. the right to opt-out. The US is an opt-out system, meaning that data subjects are automatically opted-in to share their personal information when signing up for a social media site, for example. However, the EU essentially is an opt-in system where controllers must first receive consent to process the users' data. Along with California, if New York and Massachusetts consumer privacy Act passes, they too will have the same rights guaranteed under the GDPR. Even with Washington's privacy bill failing for the third year in a row this year, it is expected to be brought back up again.[142]

Since the adoption of CCPA, 30% of U.S. Companies reported compliance, with 18% expected to be by the end of the year. Another 27% will comply by the following year. In total,

[141]Sam Dean, "California Voters Approve Prop. 24, Ushering in New Rules for Online Privacy." Los Angeles Times. November 04, 2020. Accessed June 19, 2021. https://www.latimes.com/business/story/2020-11-03/2020-california-election-tracking-prop-24.
[142]Sarah Rippy, "US State Privacy Legislation Tracker." US State Privacy Legislation Tracker. Accessed June 19, 2021. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.

over 70% of companies were willing to comply with the CCPA compared to the 12% who had no plans to comply with the CCPA.[143] This may be due to various reasons as California, on its own, is the fifth-largest economy in the world and many big tech companies are in Silicon Valley. With the Safe Harbor Privacy, the predecessor to the Privacy Shield, over 4,000 US companies were thought to have adopted the necessary regulations to have EU data subject's information.[144] Both the Safe Harbor and the Privacy Shield have been voluntary opt-in for U.S. companies. Hence companies that have joined the U.S.-EU data-sharing framework have had to update their data protection policies to meet some measures required by the EU, may have no problem complying with the CCPA.

Currently in India, the Information Technology Act, 2000 (IT Act) groups all the legislation dealing with e-commerce and cybercrimes matters. On the heels of the *K.S. Puttaswamy vs. Union of India* (2017) ruling, which established the right to privacy, the Indian government created an expert committee to conceive India's data protection framework. The current draft contains an even stronger aspect than its trading partner European Union's General Data Protection Regulation. Individuals can have their data be erased directly by communicating with the Data Protection Authority rather than putting in a request from the organization that houses the data. The PDP also sets the age threshold for being considered a child higher than the GDPR. Where the GDPR regulates that the parent or guardian must give consent with children under the age of 16, India's privacy bill caps at anyone under the age of 18 requiring consent.

Since the PDP has stalled for the past few years, one of the main questions that remain is the tech industry's reaction to a changing data protection landscape in India. While the big tech

[143] Please see Figure 1 on the percentage of companies and the compliance numbers in the United States as of October 2019.
[144] Ibid.

giants have agreed to comply with the proposed legislation, many pro-business advocates in India are raising issues with the Bill. The Internet and Mobile Association of India ((IAMAI) has raised questions about whether the bill will be practical in protecting the privacy of 1.3 billion Indians, and what will be the cost on smaller businesses. There are hefty penalties for non-compliance, reaching up to $ 700,000 or 2% of a company's global revenues. The U.S.-India Business Council (USIBC) has also raised concerns on the Intellectual Property Rights of businesses. Since insights are drawn from the collection of personal information, and the data is anonymized, meaning that data that could identify an individual is removed, may still be considered personal data and can be collected by the Data Protection Authority.[145]

Furthermore, the independence of the Data Protection Authority, who is not only selected by the Indian government but who can also be removed by them is unsettling for businesses who say there may be a conflict of interests. Additionally, the bill requires data fiduciaries, including companies or individuals who decides the means and purpose of processing personal data to store a copy of it on a local server in India which may also be accessible to Indian authorities. Finally, India has relatively limited experience with such a data protection bill, businesses are worried about the ability of the Indian government to manage all the undertakings that this bill has outlined.

Issues prevalent to Data Protection and Privacy in the U.S. and India

From the previous case studies where, recent legislation was either proposed or passed, there is evidence of a shift to a more human rights approach. The human rights approach not "only recognizes a fundamental right to privacy, but also acknowledges the interrelationship

[145] "Industry Bodies Concerned over Data Protection Bill, Say It 'compromises' on Privacy." The Economic Times. December 12, 2019. Accessed July 30, 2021. https://economictimes.indiatimes.com/tech/internet/industry-bodies-concerned-over-data-protection-bill-says-it-compromises-on-privacy/articleshow/72494630.cms?from=mdr.

between privacy and the right of individuals to exercise their other rights and freedoms with autonomy and dignity. Further, the human right to privacy must be supported by legislation that renders the right effective and realizable."[146] However, data protection regulations have implications for international trade and development and involve multiple stakeholders. To remain competitive, countries like the US and India benefit from increased data flow and restricting it can have damaging effects.

For India, that effect is heightened. They are currently expected to outpace Japan to become the third-largest economy by 2030 and are the world's largest democracy. While India has grown significantly within the last 20 years, experiencing exponential growth, the country experiences significant economic wealth gaps and lacks political, cultural, and social change. It ranks 116 out of 174 countries on World Bank's annual Human Capital Index. The index measures health and education standards in a country and its ability to provide its citizens with economic growth and access to education. India wants to be able to compete with the most prominent markets but also must answer to the changes at home. Given all these things, India wants to maintain its economic progress. It would be affected like the U.S. if policies hindered the economic openness and free flow of information, but they also see the benefits of partnerships if they can adopt data protection and privacy policies like most of the world. India is still one step ahead of the US by adopting privacy as a fundamental right in its constitution. The approach of the U.S., which has traditionally followed a Lazier fairness to data protection, has been deemed inadequate enough to protect the privacy and thus the personal data of data

[146] "Two Sides of the Same Coin – the Right to Privacy and Freedom of Expression." Privacy International. Accessed June 19, 2021. https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression.

subjects. The U.S.'s lack of recognition to explicitly state the right to privacy is divergent from today's norms, expectations and may harm the economic interest of the world's superpower.

With the Indian government expected to be exempted from the data privacy legislation, privacy activist is concerned that about the overreach of the Indian government, the growth of surveillance activities, and the recent news that the Indian government is planning on creating a single centralized facial recognition database which the country's law enforcement agencies will have access to. In the United States, big tech companies hold considerable influence in the making of legislation and the increased normalization of mass surveillance by the government. Both countries are battling the issue of national security vs. privacy.

Recommendations

The European Union holds all third countries like India and the U.S., and their tech company that processes the data of anyone residing in the EU to its strict privacy standards. “Data-driven global interactions and digital dependencies necessitate” the need for a privacy and data protection legislation.[147] Countries are quickly beginning to adopt similar approaches to the General Data Protection Regulation as the main framework. However, many of these regulations suffer from a shortage of mechanisms for proper protection. For the world to truly move towards harmonizing their views on data protection and provide adequately for the right to privacy but also other fundamental rights, they must:

- Look towards the OECD policy framework as guidance on certain principles and implementation methods since it resembles the GDPR.

[147] Sangeeta Mahapatra, “Digital Surveillance and the Threat to Civil Liberties in India.” German Institute of Global and Area Studies (GIGA), 2021. http://www.jstor.org/stable/resrep31794, 2.

- Ensure that rights and obligations, and consequences are outlined in data protection regulations.
- Promote more robust safeguards like encryption and anti-malware security and anonymization.[148]

Conclusion

In the age of digital transformation, companies rely even more on the use of personal data to extract important narratives that can drive business growth. Often times not paying attention to the fine print and terms of service when signing up for a website, the personal data of individuals are left on unsecured servers and transmitted to third-party companies who do with what they want with it. The recent pandemic has brought about an even more giant wave of internet usage. In a Pew research study done in August 2020, about 89% of 18-to-29-year-old reported from the 34 countries surveyed that they used the internet or had a smartphone.[149] Thirty of the 34 countries surveyed also had the most users on social media platforms. Consumers also looked to the internet to shop for necessities when physical businesses had to close. More so, the tracking of health information during the pandemic has heightened fears with extracting and safely transferring data. Government agencies often go overboard in collecting and using surveillance technology like facial recognition in the name of national security.

Recognizing the right to privacy in today's world means protecting personal information. This means adopting an all-inclusive data protection legislation and creating accountability

[148] Anonymization is defined as removing the person's personally identifiable information, ensuring the data cannot be associated with an individual.

[149]Shannon Schumacher, and Nicholas Kent. "8 Charts on Internet Use around the World as Countries Grapple with COVID-19." Pew Research Center. July 27, 2020. Accessed December 05, 2021. https://www.pewresearch.org/fact-tank/2020/04/02/8-charts-on-internet-use-around-the-world-as-countries-grapple-with-covid-19/.

practices for companies, organizations, and even governments. The protection of the right to privacy also guarantees other rights, including the right to freedom of expression as described in Article 19 of the Universal Declaration of Human Rights and the right to, Article 7 which denotes the right not to be discriminated against. Data Protection should be comprehensive and transparent, or it will result in gaps, as shown in the case studies where a lack of security measures and laws endanger the personal data of individuals who are susceptible to fraud and theft. Organizations are also vulnerable to data breaches, which can negatively impact businesses overall. Regulations must include the rights of users, and observatory body and the right to opt-out, especially as auto-decision making practices can lead to discrimination.[150]

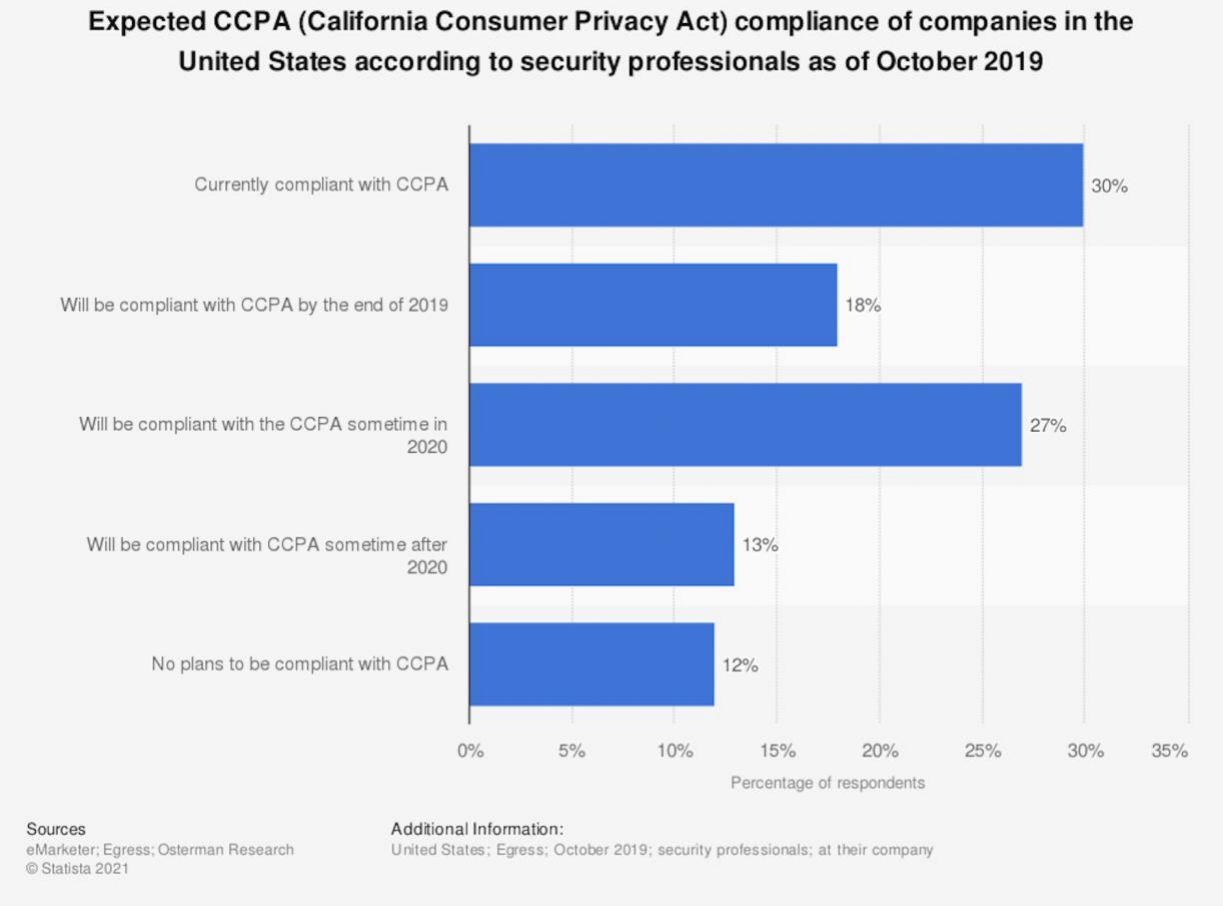
Recently, China adopted its own data protection legislation joining a multitude of other countries that have adopted privacy legislation within the last few years. In Europe, international transfer of personal data such as census data from Portugal has been put on pause to the U.S. because of the court decision in 2020 on the failure of the Privacy Shield to live up to expectations by the EU.

Establishing national legislation would align countries with one another, remove incoherent data practices, create a global norm around data governance, and improve trade.

[150]Mark MacCarthy, "Fairness in Algorithmic Decision-making." Brookings. December 11, 2019. Accessed December 05, 2021. https://www.brookings.edu/research/fairness-in-algorithmic-decision-making/.

Appendix

Figure 1



Source: Statista

Bibliography

Journals and Books

Birnhack, Michael D. "The EU Data Protection Directive: An engine of a global regime." Computer Law & Security Review 24, no. 6 (2008): 508-520.

Debatin, Bernhard “Ethics, Privacy, and Self-Restraint in Social Networking” In Online: Perspectives on privacy and self-disclosure in the social web, eds. Trepte, Sabine, and Leonard Reinecke, 47-60. Springer Science & Business Media, 2011.

Determann, Lothar, and Chetan Gupta. "India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018." Berkeley J. Int'l L. 37 (2019): 481.

Goddard, Michelle. "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact." International Journal of Market Research 59, no. 6 (2017): 703-705.

Greenleaf, Graham. "The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108." International Data Privacy Law 2, no. 2 (2012): 2011.

Greenleaf, Graham. "Global data privacy laws 2019: 132 national laws & many bills." 157 Privacy Laws & Business International Report. February 8, 2019.

International Organization of Migration. The IMO Data Protection Manual, 2011, statement. Switzerland: International Organization of Migration, 2011.

Kulhari, Shraddha. "Data Protection, Privacy and Identity: A Complex Triad." In Building-Blocks of a Data Protection Revolution: The Uneasy Case for Blockchain Technology to Secure Privacy and Identity, 23-37. Baden-Baden, Germany: Nomos Verlagsgesellschaft MbH, 2018. Accessed June 18, 2021. http://www.jstor.org/stable/j.ctv941qz6.7.

Kuner, Christopher. "An international legal framework for data protection: Issues and prospects." Computer law & security review 25, no. 4 (2009): 307-317

La Rue, Frank. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. Report to the United Nations General Assembly Human Rights Council. A/HRC/23/40 (2012)

Mahapatra, Sangeeta. “Digital Surveillance and the Threat to Civil Liberties in India.” German Institute of Global and Area Studies (GIGA), 2021. http://www.jstor.org/stable/resrep31794.

Misra, Prakhar. "Lessons from Aadhaar: Analog aspects of digital governance shouldn’t be overlooked." Pathways for Prosperity Commission Background Paper Series 19 (2019).

Moshell, Ryan. "And then there was one: The outlook for a self-regulatory united states amidst a global trend toward comprehensive data protection." Tex. Tech L. Rev. 37 (2004): 357-432.

Niebel, Crispin. "The impact of the general data protection regulation on innovation and the global political economy." Computer Law & Security Review 40 (2021):1-15.

UNCTAD (United Nations Conference on Trade and Development). "Data Protection Regulations and International Data Flows: Implications for Trade and Development." (2016).
US Congressional Research Service. Data Protection Law: An Overview

Websites

"2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020." HIPAA Journal. March 03, 2021. Accessed July 10, 2021. https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/.

Ahmad, Tariq. National Parliaments: India. February 01, 2017. Accessed June 16, 2021. https://www.loc.gov/law/help/national-parliaments/india.php#Structure.

"Art. 20 GDPR - Right to Data Portability." GDPR.eu. July 23, 2020. Accessed June 14, 2021. https://gdpr.eu/article-20-right-to-data-portability/.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information." Pew Research Center: Internet, Science & Tech. August 17, 2020. Accessed June 11, 2021. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

"California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General. July 14, 2021. Accessed July 20, 2021. https://oag.ca.gov/privacy/ccpa.

Chaturvedi, Aditi. "GDPR and India: A Comparative Analysis." Centre for Internet & Society. October 17, 2017. Accessed November 30, 2021. https://cis-india.org/internet-governance/blog/gdpr-and-india-a-comparative-analysis.

"Cost of a Data Breach Study." IBM. Accessed June 18, 2021. https://www.ibm.com/security/data-breach.

Council of Europe, Convention for the Protection of Individuals concerning the Automatic Processing of Individual Data, 28 January 1981, ETS 108, available at: https://www.refworld.org/docid/3dde1005a.html [accessed 19 December 2020

Data Protection." European Data Protection Supervisor - European Data Protection Supervisor. November 11, 2016. Accessed October 20, 2020. https://edps.europa.eu/data-protection_en

Data Protection and Privacy Legislation Worldwide." UNCTAD. Accessed April 01, 2021. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide.

Dean, Sam. "California Voters Approve Prop. 24, Ushering in New Rules for Online Privacy." Los Angeles Times. November 04, 2020. Accessed June 19, 2021. https://www.latimes.com/business/story/2020-11-03/2020-california-election-tracking-prop-24.

"Does the GDPR Apply to Companies outside of the EU?" GDPR.eu. February 13, 2019. Accessed June 08, 2021. https://gdpr.eu/companies-outside-of-europe/.

Doshi, Vidhi. "Analysis | A Security Breach in India Has Left a Billion People at Risk of Identity Theft." The Washington Post. February 25, 2018. Accessed June 16, 2021. https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/.

European Union, Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02, available at: https://www.refworld.org/docid/3ae6b3b70.html [accessed 18 June 2021]

"Factbox: Reaction after EU Court Strikes down Transatlantic Data Transfer Deal." Reuters. July 16, 2020. Accessed May 01, 2021. https://www.reuters.com/article/us-facebook-privacy-eu-reaction-factbox/factbox-reaction-after-eu-court-strikes-down-transatlantic-data-transfer-deal-idUSKCN24H1QV.

Gill, Prabhjote. "India's Three Main Surveillance Projects NATGRID, CMS and NETRA Have Been Directed to Stop Collecting Data Citing Breach of Privacy." Business Insider. December 02, 2020. Accessed June 20, 2021. https://www.businessinsider.in/tech/news/indias-three-main-surveillance-projects-natgrid-cms-and-netra-have-been-directed-to-stop-collecting-data-citing-breach-of-privacy/articleshow/79529256.cms.

Gopalakrishnan, Manasi. "India's Personal Data Privacy Law Triggers Surveillance Fears: DW: 11.11.2020." DW.COM. 2020. Accessed June 20, 2021. https://www.dw.com/en/indias-personal-data-privacy-law-triggers-surveillance-fears/a-55564949.

Greenberg, Pam. 2020 Consumer Data Privacy Legislation. January 17, 2021. Accessed June 14, 2021. https://www.ncsl.org/research/telecommunications-and-information-technology/2020-consumer-data-privacy-legislation637290470.aspx.

"Guidance on the Protection of Personal Identifiable Information." U.S. Department of Labor Seal. Accessed June 18, 2021. https://www.dol.gov/general/ppii.

Hoofnagle, Chris Jay, Woodrow Hartzog, and Daniel J. Solove. "The FTC Can Rise to the Privacy Challenge, but Not without Help from Congress." Brookings. August 08, 2019. Accessed June 13, 2021. https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/.

In Committee. Accessed June 15, 2021. https://www.house.gov/the-house-explained/the-legislative-process/in-committee.

Johnson, Joseph. "Biggest Online Data Breaches Worldwide 2021." Statista. May 25, 2021. Accessed June 16, 2021. https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/.

Kajal, Kapil. "India's Tech Industry up in Arms over Proposed Data Privacy Law." Nikkei Asia. January 10, 2020. Accessed June 20, 2021. https://asia.nikkei.com/Business/Business-trends/India-s-tech-industry-up-in-arms-over-proposed-data-privacy-law.

Kelligrant. "Identity Theft, Fraud Cost Consumers More than $16 Billion." CNBC. February 01, 2017. Accessed June 18, 2021. https://www.cnbc.com/2017/02/01/consumers-lost-more-than-16b-to-fraud-and-identity-theft-last-year.html.

Lok Sabha Secretariat Parliamentary Forum (April 4, 2014). “How a Bill Becomes an Act?”, New Delhi, No.20. Accessed on June 19, 2021. < http://164.100.47.194/our%20parliament/How%20a%20bill%20become%20an%20act.pdf>

MacCarthy, Mark. "Fairness in Algorithmic Decision-making." Brookings. December 11, 2019. Accessed December 05, 2021. https://www.brookings.edu/research/fairness-in-algorithmic-decision-making/.

Menn, Joseph. "WhatsApp Sues Indian Government over New Privacy Rules - Sources." Reuters. May 26, 2021. Accessed June 20, 2021. https://www.reuters.com/world/india/exclusive-whatsapp-sues-india-govt-says-new-media-rules-mean-end-privacy-sources-2021-05-26/.

Miller, Claire Cain. "Revelations of N.S.A. Spying Cost U.S. Tech Companies." The New York Times. March 21, 2014. Accessed June 18, 2021. https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

O’Connor, Nuala. "Reforming the U.S. Approach to Data Protection and Privacy." Council on Foreign Relations. January 30, 2018. Accessed June 16, 2021. https://www.cfr.org/report/reforming-us-approach-data-protection.

Panday, Jyoti. "India's Supreme Court Upholds Right to Privacy as a Fundamental Right-and It's About Time." Electronic Frontier Foundation. October 11, 2017. Accessed June 16, 2021. https://www.eff.org/deeplinks/2017/08/indias-supreme-court-upholds-right-privacy-fundamental-right-and-its-about-time.

Paul, Kari. "Americans' Data Is worth Billions - and You Soon Might Be Able to Get a Cut of It." MarketWatch. October 09, 2018. Accessed June 19, 2021. https://www.marketwatch.com/story/americans-data-is-worth-billions-and-you-soon-might-be-able-to-get-a-cut-of-it-2018-10-09.

Perlroth, Nicole. "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack." The New York Times. October 03, 2017. Accessed December 20, 2020. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Rippy, Sarah. "US State Privacy Legislation Tracker." US State Privacy Legislation Tracker. Accessed June 19, 2021. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/.
Smith, Aaron. "Americans and Cybersecurity." Pew Research Center: Internet, Science & Tech. August 17, 2020. Accessed June 18, 2021. https://www.pewresearch.org/internet/2017/01/26/americans-and-cybersecurity/.

Schumacher, Shannon, and Nicholas Kent. "8 Charts on Internet Use around the World as Countries Grapple with COVID-19." Pew Research Center. July 27, 2020. Accessed December 05, 2021. https://www.pewresearch.org/fact-tank/2020/04/02/8-charts-on-internet-use-around-the-world-as-countries-grapple-with-covid-19/.

The Council of Economic Advisers. 2018. The Cost of Malicious Cyber Activity to the U.S. Economy. Washington, DC: Executive Office of the President, February 2018.Accessed June 16, 2021. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

THE PERSONAL DATA PROTECTION BILL, 2018 (India) .< https://www.meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf>

"The World's Most Valuable Resource Is No Longer Oil, but Data." The Economist. May 6, 2016. Accessed May 01, 2021. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.

"Third Countries." General Data Protection Regulation (GDPR). August 13, 2020. Accessed June 19, 2021. https://gdpr-info.eu/issues/third-countries/.

"Two Sides of the Same Coin – the Right to Privacy and Freedom of Expression." Privacy International. Accessed June 19, 2021. https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression.

United States. Dept. of Health and Human Services. HC3: Sector Alert. Picture Archiving Communication Systems (PACS) Vulnerabilities. Report: 202106291300. HHS Office of Information Security: Health Sector Cybersecurity Coordination Center (HC3), June 29, 2021.Accessed July 10, 2021.https://www.hhs.gov/sites/default/files/pacs-vulnerabilities.pdf

"What Is Considered Personal Data under the EU GDPR?" GDPR.eu. February 13, 2019. Accessed June 06, 2021. https://gdpr.eu/eu-gdpr-personal-data/.

"2021 Data Breach Investigations Report." Verizon Enterprise. Accessed March 21, 2021. https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pd