April 27, 2022

PSCI 180 Final Paper

Cookies and Convention: International Organizations' Influence on Data Privacy Regulations

Since its invention, the internet has become increasingly globalized and is now broadly accessible around the world. With this explosive growth, a person can access information and data on sites which originated on the other side of the globe. In many ways, this aspect of the internet has had major beneficial influences on globalization and transnational information sharing. However, this has also opened a gray area on data privacy and protection of personal data, with no firm standards or regulations. It is in this gray area that international regulations and standards of data privacy are increasingly necessary; the current state of vastly different levels in individual countries is not sustainable as the internet continues to grow. Currently, some organizations (including the European Union, the Organization for Economic Cooperation and Development, the Council of Europe, and the Asia-Pacific Economic Cooperation) have laid out standards for their member states, some of which are mandatory and others voluntary in their compliance. The European Union, with the most comprehensive and strict guidelines, has gone on to influence the regulations of many individual states and other organizations. While that has brought these standards a long way in terms of universal application, it is not yet enough. Due to the transnational nature of the internet, no individual state can set standards that all corporations, states, individuals, and groups can be expected to follow. As such the burden of protecting data by setting standards has fallen to international organizations, some of which are already involved and influence standards in other regions. However, to maintain safe internet practices in a globalized world, international organizations must facilitate a global agreement on the implementation of these standards and continue to prioritize data privacy as the internet evolves.

In the 40 years since the Internet was created, its nature has vastly changed and evolved to be what it is known as today. What began as a small computer network for the U.S. Department of Defense has since expanded into a global infrastructure offering industrial, commercial, and government uses, connecting people from across the globe (University Systems of Georgia). The internet has been agreed upon by most to be a tool for economic and social development, as an increasing amount of research, communication, and business is done online. The internet has promoted the globalization of many sectors, including businesses and non-profits. Organizations can use the internet for informing, interacting, and fundraising at a level that can access more people (Yasin, 150). However, considering the roles the internet can aid organizations in, it is even more crucial that these organizations, and others, realize the importance of the trust their employees, customers, and stakeholders place in protecting data privacy if they are to continue communicating personal data across the internet, as is done in online donation services, for example.

While the internet has created many development opportunities, it has also raised concerns about the issue of data privacy. As the availability and use of the internet have become more widespread, it has also become easier for personal data to be spread, misused, and abused (Klosek, 8). The internet may be a widely useful source of information on assorted topics, it is also a vast source of information on individuals. There are many methods of data collection, ranging from the more obvious user inputs to the more obscure use of cookies, all of which provide websites with data they then collect on their users. This data can include a person's name, location, financial information, contact information, organizational membership, political and religious beliefs, health information, biometric data, relationship information, government identification documents, and identifying traits such as race, gender, and ethnicity. Personal data on the internet can be put at risk of being compromised through the mass storage and selling of

information by organizations and corporations if the most secure methods of storing are not followed and corporations are left unchecked in selling data to other companies for means of advertising or developing. To address this issue, the European Union began setting standards to place limits on the collection and use of personal data from the government level. The EU's standards have become one of the most strict and comprehensive, especially in comparison to others, such as the United States' preference for methods of self-regulation. With the differences in standards and the EU's accusations of the US and others' inadequate protections, it is difficult for any firm conclusions on international standards to be made (Klosek,13 –21). The issue arises then with the fact that the internet does not follow any national borders, so regulations and standards for the nature of the internet must also not vary based on national location, as it becomes difficult to determine which guidelines a transnational corporation, organization, or group should follow for their online services.

Leading organizations in setting regulations regarding data privacy are the Council of Europe, the Organization for Economic Cooperation and Development, the European Union, the Asia-Pacific Economic Cooperation, and the United Nations. The global idea for the protection of privacy began with the Universal Declaration of Human Rights of 1948 and the International Covenant on Civil and Political Rights of 1966, which helped develop standards of data privacy protections in the 1970s (Kuner, 9). During the 1970s, the first data protection laws began being passed in European countries, regulating transborder data movement. In 1980, the OECD made the first global attempt with their Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, a non-binding set of principles member states may voluntarily enact (Kuner, 16), and by 1981, the Council of Europe passed Convention 108. This Convention is often referred to as the first international treaty that specifically addresses data protection, and has since been ratified by forty-two countries, mostly in Europe, but is also open to signature by non-

member states, although none have thus far (Kuner, 18). Convention 108, in the form it was passed, made too many allowances for differing standards that would excuse certain data transfers from following the regulations laid out. Though Convention 108 is an important regulation that began the standards of privacy in a digital age, its passage in 1980 makes it outdated and irrelevant for the current state of technology.

In addition to Convention 108, the most influential legal data protection rules originate from the European Union. The EU began with their Data Protection Directive, restricting foreign data transfers based on the non-Directive following countries' levels of data protection, reliant on the determinations of the European Commission (Jones and Tahri, 635), as well as regulating the processing of personal data (Jones and Tahri, 631). More recently, the EU has also enacted their "ePrivacy Directive" and "ePrivacy Amendment Directive," aiming to mandate the confidentiality of communications and the rules around tracking and monitoring ("ePrivacy"), as well as regulate the use of cookies (Jones and Tahri, 630). The EU's directives make a stronger attempt than previous policies to protect personal data during transfers and processing and against the use of collected data.

Outside of Europe, in 2004, the Asia-Pacific Economic Cooperation group agreed to the APEC Privacy Framework, a set of guidelines that members may voluntarily implement, intending to protect personal data transferred outside of member states (Kuner, 20). In addition to regulations established by organizations, several voluntary and private-sector guidelines attempt to regulate data movements, such as the US-EU Safe Harbor framework, voluntary standards for US-based organizations that import personal data from the EU, and the privacy standards of the International Organization for Standardization (Kuner, 23-24). Though these are not mandatory regulations, some can be legally binding to adoptees and have become widely used to create unofficial standards of regulation for corporations.

As the first global attempt at data privacy regulations, the OECD Privacy Guidelines, despite being non-binding and non-enforceable in member states, are influential. Most OECD member states have used the OECD guidelines when drafting their national privacy laws. Canada, for example, enforces a Personal Information Protection and Electronic Documents Act, and in line with the OECD principles, requires all data collection purposes to be identified and disclosed (Greenberg, 20-21). Additionally, despite the regional limitations of the EU's directives, and the nonexistence of global regulations, many states have taken to modelling their domestic data protection laws after those of the EU. In more recent years, the occurrence of data privacy laws outside of the EU has increased, from thirty-nine in 2012 to sixty-six in 2017, the majority of which followed EU guidelines, and most of the laws implemented EU principles about supporting legal reparations, data deletion, data protection agencies, and restrictions on data exports because of laws in the recipient country (Greenleaf, 1). This increasing rate of adoption of European standards in many of the top GDP earning states indicates the beginning of a trend towards a majority global standard and agreement based on the European standards.

In 2018, the EU put into effect the General Data Protection Regulation, giving all EU citizens greater individual access rights to their data. At the time of enactment, many were concerned about how these regulations would be affected by the differences between the EU and US standards, as the EU guidelines would now apply to non-EU corporations that have EU consumers and users. Although many argued the GDPR would cause hardship for US-based entities, in analyzing its policies, it is clear it also incorporates several of the few American data privacy laws, including the ideas of "privacy by design" and security breach notifications, as well as deterrence-based fines (Rustad and Koenig, 6). Furthermore, with the weak data laws in the US, and the strictly enforced laws of the EU, many US-based organizations, facing the threat of expensive fines or ending business within the EU, are finding it easier to always apply the

strictest global standards rather than differentiating based on location (Rustad and Koenig, 23), leading to the agreement to the US-EU Safe Harbor Framework. While the GDPR is not an international standard, it has managed to create a hybrid of American and European legal practices (Rustad and Koenig, 46), a fact that will make the bridging of data protection differences that much easier and allow the potential for the GDPR to eventually become the international standard as most corporations move to follow the strongest guidelines everywhere rather than following several regionally.

As they stand, individual, state-level standards are not enough to protect all internet users' data. Depending on the state, policies can be based on the universal human rights to privacy, or economically motivated (Kuner, 27). With constant ongoing discussions between the various actors in data privacy, and the ever-evolving nature of technology, it is difficult to say for sure which way data privacy regulations are due to evolve, or even ways they need to adapt, but in analyzing existing policies, some issues are clear that need resolving. With existing policies and regulations, key issues are the legal nature of the different approaches, the basis of a regulation as geographic versus organizational and how it factors into types of approaches, compliance, and enforceability, as well as the differences in the default definition in standards. Considering some policies address data privacy from the perspective of human rights while others consider it from economic terms (Kuner, 27), for an international standard to be worked towards, there needs to be a consensus on whether data privacy is a universal right that needs to be protected. Additionally, the geographic versus organizational approaches make it difficult to reach an international agreement as regional standards tend to protect against location-based risks, while organizational approaches think about risks posed by the receiving groups (Kuner, 28). The compliance and enforceability of a standard is another major issue to consider when thinking about global standards as the varying standards and requirements make it difficult for

both corporations and individuals to manage (Kuner, 28 – 29). While the internet has allowed individuals to be more directly involved in their personal data transfers, this increasing complexity of regulation has only made it more difficult for individuals to know what they are consenting to when transferring data, leading to greater risks of data being compromised. Finally, the vastly different standards around the world define different levels of default positions in data privacy, some taking the position that there should be limited regulations on data, such as under the OECD, while others prefer stronger guidelines on data movement to grant broader protection, such as the EU (Kuner, 30). With this vast difference, in a more globalized world that relies on the internet for economic and social development, that development is put at risk by the variance of restrictions that can slow down data movement that would otherwise benefit economies and societies.

As technology and the internet evolves, there must be a recognition of the importance of data privacy protections at high government levels, as only then will international agreements be able to be made. Additionally, it is important for regulations focusing on advertisement targeting to be made, in addition to data movement regulations. Most recently, as they have begun to fully understand this importance, the EU passed the Digital Services Act, a law aimed to address the harms of social media, but also stop using personal data to target online ads based on ethnicity, religion, and sexual orientation (Satariano). As a new law, it is unclear how effective this law will be, but it is a step in the right direction. If it is to follow in the direction of the GDPR's effective enforcement (Erickson, 888), there is the potential for this new law to further protect personal data from being sold by companies, such as Google, Facebook, and TikTok, or used to target advertisements towards users based on their data.

International organizations including the OECD, the EU, APEC, and the Council of Europe have played a significant role in the process of establishing data privacy regulations over

the past forty to fifty years. The global nature of the internet has benefited the world in many ways, allowing for broader globalization and reach of corporations, organizations, groups, and individuals. Without the internet, society and the economy would not be where they are today. With all the benefits the internet has brought the world, however, the world has seen the ways technology companies have begun to use the dependence individuals have on the internet to their advantage, often abusing their access to personal user data. Allowing these trends of data compromising is dangerous, putting individuals at risk of sensitive information being shared in the wrong places or with the wrong people. Privacy is a right, as laid out by the United Nations, and while their declaration at the time was unaware of the future of online data privacy needs, the idea still applies. Because the internet is global in its reach and uses, no individual state can be left to enforce regulations on the internet and internet corporations to protect individuals. Instead, it is the responsibility of international organizations to provide a forum for governments to come together to set standards that will protect all internet users worldwide, beyond those that currently exist. The internet and technology will only continue to evolve, and international organizations must continue to prioritize data privacy at a global level for all states to agree to these standards and protect the personal data of individual users.

Works Cited

Board of Regents of the University System of Georgia. "A Brief History of the Internet" *Online Library Learning Center*, University System of Georgia, www.usg.edu/galileo/skills/unit07/internet07_02.phtml#:%7E:text=January%201%2C%201983%20is%20considered,to%20communicate%20with%20each%20other. Accessed 28 Apr. 2022.

"ePrivacy Directive." *European Data Protection Supervisor*, European Union, edps.europa.eu/data-protection/our-work/subjects/eprivacy-directive_en. Accessed 28 Apr. 2022.

Erickson, Abigayle. "Comparative Analysis of the EU's GDPR and Brazil's LGPD: Enforcement Challenges With the LGPD." *Brooklyn Journal of International Law*, vol. 44, no. 2, 2019, pp. 859–88. *Brooklaw*, brooklynworks.brooklaw.edu/bjil/vol44/iss2/9/?utm_source=brooklynworks.brooklaw.edu%2Fbjil%2Fvol44%2Fiss2%2F9&utm_medium=PDF&utm_campaign=PDFCoverPages.

Greenberg, Anastasia. "Inside the Mind's Eye: An International Perspective on Data Privacy Law in the Age of Brain-Machine Interfaces." *SSRN Electronic Journal*, vol. 29, no. 1, 2018, pp. 79–122. *Crossref*, doi:10.2139/ssrn.3180941.

Greenleaf, Graham. "'European' Data Privacy Standards Implemented in Laws Outside Europe." *149 Privacy Laws & Business International Report 21–23*, 2017. *SSRN*, ssrn.com/abstract=3096314.

Jones, Richard, and Dalal Tahri. “An Overview of EU Data Protection Rules on Use of Data Collected Online.” *Computer Law & Security Review*, vol. 27, no. 6, 2011, pp. 630–36. *Crossref*, doi:10.1016/j.clsr.2011.09.003.

Klosek, Jacqueline, editor. *Data Privacy in the Information Age*. Quorum Books, 2000. *EBSCO*, search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=69194&site=ehost-live&ebv=EB&ppid=pp_7.

Kuner, Christopher. “Regulation of Transborder Data Flows Under Data Protection and Privacy Law: Past, Present, and Future.” *SSRN Electronic Journal*, 2010. *Crossref*, doi:10.2139/ssrn.1689483.

Rustad, Michael L., and Thomas H. Koenig. “Towards a Global Data Privacy Standard.” *Florida Law Review*, vol. 71, no. 2, 2019, pp. 365–453. *EBSCO*, eds.s.ebscohost.com/eds/detail/detail?vid=0&sid=c5b5ced0-c1a3-4782-9cb3-f9d567f0a8ce%40redis&bdata=JnNpdGU9ZWRzLWxpdmU%3d#db=edo&AN=137238347.

Satariano, Adam. “E.U. Takes Aim at Social Media’s Harms With Landmark New Law.” *The New York Times*, 23 Apr. 2022, www.nytimes.com/2022/04/22/technology/european-union-social-media-law.html.

Yasin, Ozcelik. “Globalization and the Internet: Digitizing the Nonprofit Sector.” *Journal of Global Business Issues*, vol. 2, no. 1, 2008, pp. 149–52. *EBSCO*, search.ebscohost.com/login.aspx?direct=true&db=buh&AN=31381054&site=eds-live.