The Evolving Landscape of International Consumer Data Privacy Compliance

Dr. Mark Pisano
Department of Business Information Systems
Southern Connecticut State University
pisanom1@southernct.edu

Robert A. Smith, Esq., MBA
Department of Management and International Business
Southern Connecticut State University
smithjrr1@southernct.edu

Kauther S. Badr, Esq., MBA
Department of Management and International Business
Southern Connecticut State University
badrk1@southernct.edu

Abstract

The internet and the world wide web have grown substantially and become a significant part of everyday life, even more so since the Covid-19 pandemic. Societal reliance on the internet and the world wide web has generated increasing concerns about data privacy. The rise in usage has also increased the amount of data—user data— input into apps, programs, and websites. There is an increased risk that user data could be intentionally or unintentionally made available to third parties for purposes unanticipated by the user. Companies regularly collect and use user data for commercial purposes such as target marketing, branding campaigns, or to inform research and product development. user data has become highly valuable, creating a need to regulate the activities surrounding its collection, storage, and use. This trend has also prompted global governmental involvement. Most notably, the European Union enacted the ePrivacy Regulation (ePR) and the General Data Protection Regulation (GDPR). These laws significantly impact how user data is collected, stored, and shared and have become drivers for considerable change in business practices surrounding user data. Furthermore, the evolving legal landscape has required website operators to change how they utilize internet cookies— electronic files that collect and store user data, allowing website owners to track user behavior. Recently, there has been a large-scale push to change how the world wide web operates, which includes the elimination of the use of cookies to ensure user privacy. This paper examines the effect of recent global privacy regulations and provides suggestions as to what organizations can do to keep up with the changing legal landscape. Potential changes to data gathering on the world wide web and the technical issues these changes may bring are also explored.

Introduction

The internet has accelerated globalization for businesses and allowed for efficiencies in commerce. Companies use the internet to sell their products, network, conduct client meetings, and much more. During the Coronavirus pandemic, courts throughout the United States even used the internet to conduct official court business. The pandemic has caused most societies to become dependent upon the internet for daily and basic life needs, which has caused a significant increase in the amount of commerce that is taking place over the internet.

Consumers use the internet to engage in commerce by making purchases and even obtaining medical services through virtual meetings. The rise of social media in many societies also causes consumers to be on the internet and engage with businesses, marketers, influencers, and the like. Due to the way people now leverage the internet every single day for multiple purposes, there are robust and thriving depositories of user data available for potential use or misuse.

user data, sometimes known as an internet footprint, can consist of personally-identifying information like a consumer's name, date of birth, and home address. This data can include but is not limited to consumers' credit card info, purchase history, preferences, likes, and dislikes based on browsing history and habits. Given the data's valuable nature, a growing industry focuses on its collection, analysis, distribution, and sale. (Klosowski, 2021). Data collection companies may also analyze the data and sell valuable analytics, which allows a business to interpret it and make data-informed business decisions quickly. Consumers worldwide have become understandably concerned about their privacy and how organizations collect, store, sell, and use their data.

A notable government intervention that has far reach comes from the European Union enacting the ePrivacy Regulation (ePR) and, more recently, the General Data Protection Regulation (GDPR). Other large jurisdictions, such as China and Brazil, have followed suit with regulations that seriously impact user data collection, storage, and sharing (Rudo & Reagan, 2021). These laws have been change agents in how the world wide web operates legally and technically. One of the most significant impacts of the European laws has caused website operators to change how they handle and utilize internet cookies. While these mini files are purportedly intended to make web browsing a better experience for consumers, they also collect and store user data and allow website owners to track user behavior. As such, it is no surprise that there has been a large-scale push to change how the world wide web operates and eliminate the use of cookies to ensure user privacy.

What are Internet Cookies?

Cookies are small text files used by a web browser when visiting websites, stored on a user's computer, and are intended to "enhance" the user's web browsing experience. These text files have unique identification tags tied to the website and are used to store information about the website and the interaction between the user and the site. Some examples of the types of information that cookies stores are log on and off transactions, preferences, and the last location on the site. The purpose of a cookie was initially intended to help create a more efficient and meaningful user experience. As discussed in more detail below, there are two major types of cookies: session cookies and persistent cookies.

Session Cookies

Session cookies are small, transient text files that store and utilizes the information necessary for interactions while visiting a website. They are aptly named because they are created on the website and have a short life span, lasting only as long as a user's visit or "session" on a website. Since session cookies are specifically used for the singular visit to the website, they are deleted once the session has been completed. Privacy concerns and risks associated with these cookies should be relatively low. The purpose and function of session cookies revolve more around how a website operates, i.e., how smoothly the user can navigate from page to page, rather than collecting user

data. Consumers would become quickly frustrated if session cookies did not exist. For example, when browsing an online store, session cookies allow the consumer to like certain products to come back and view later or put items in the electronic shopping bin to purchase or delete selected items later.

Persistent Cookies

Unlike session cookies, persistent cookies do not have a short life span; they continue to be stored in a web browser folder for an extended period. This period is defined within the cookie itself. Additionally, the persistent cookie file is accessed and modified with every visit to the website. Persistent cookies are not required to view a website but are meant solely to gather user data, which can be construed as a privacy violation. Currently, the EU regulations heavily affect the use of persistent cookies and the user data collected therefrom. To maintain compliance with the EU regulations, organizations that use persistent cookies to collect user data must conspicuously display disclosure and consent notifications on their websites.

The disclosure and consent notifications are displayed upon a user's first visit to a website. The notification is required to inform the user of the intention to use persistent cookies and collect user data. The notice must also include where users may find the complete data use policies and the acceptance agreement. If the user accepts the data collection, the website session will begin, and the website will collect cookie data.

Cookie Profiling

Cookie profiling is a mechanism used by advertisers to track user activity across the internet. It involves the collecting of persistent cookies across multiple websites. The data are used to create a user profile, which can be highly detailed. Some of the information gathered to create this profile can include websites users visit, purchasing trends, eating habits, hobbies and interests, and even a user’s political and religious affiliations. Furthermore, it allows for tracking a user across the web and is the foundation for the privacy concerns of all internet users. As one can imagine, this data is also very valuable and oftentimes gets sold to third parties. Privacy advocates purport that it is a myth that web data collection is harmless, anonymous, and beneficial to the consumer. They believe this type of data collection leaves consumers' personal information vulnerable. Alternatively, others view web profiling as beneficial to the consumer believing it creates a personalized web browsing experience.

Google's Announcement

As the demand for stricter privacy controls has grown, Google has led an initiative to protect user data. On August 22, 2019, Google announced it would develop the Privacy Sandbox. Google is far more than a search engine and is one of the world's largest and most influential technology companies. Laws, regulations and consumer opinion can significantly impact Google's business model and revenues.

Essentially, the Privacy Sandbox is a set of open standards designed to enhance privacy on the web (Schuh, 2019). In the August 2019 announcement, Google expressed concerns about how

advertisers and other stakeholders have used current web technology beyond what it was originally intended for and that data practices do not match privacy expectations (Schuh, 2019).

Enhancing the privacy of the web is a massive undertaking that will require input from many parties, and it time will be required to develop the technology. The overarching goal is to phase out the use of internet cookies and create a world wide web that is more open and adheres to vetted standards. Google is working with the World Wide Web Consortium (W3C) to meet its goals. (Schuh, 2020).

World Wide Web Consortium

The World Web Consortium is an international community that helps to guide and develop web standards (W3C). W3C creates business and working groups to help garner community acceptance. As discussed earlier, Google is using a group facilitated by W3C to develop a community-accepted standard to increase user privacy on the web.

The joint effort led by Google is called, Improving Web Advertising Business Group. According to the group, its purpose is to "identify areas where standards and changes in the Web itself can improve the ecosystem and experience for users, advertisers, publishers, distributors, ad networks, agencies, and others and to oversee liaison with existing Working Groups and to create new Working Groups as needed" (Improving Web Advertising Business Group, 2020, para. 1). This group has been working since November 2017. This shows that Google and other stakeholders have been informally discussing the idea of a secure cookie-less web well before any worldwide announcements were made.

As of September 2022, the group comprises 374 members coming from different organizations all over the world. Google, Microsoft, Facebook, IBM, AT&T, and Amazon are just a few organizations represented within the group. The membership shows that the Privacy Sandbox and user data privacy are being taken seriously.

The work being brought forward by the W3C group has shown progress. Google announced in early 2021 that it had successfully collected thirty different proposals, five of which would begin testing in the Privacy Sandbox (Schuh, 2021). Significant and meaningful efforts are being made to create a web free of cookies.

Workarounds

Many organizations have found value in collecting consumer data. Ecommerce sites have a deep history of data collection practices, and users have been aware of it for some time now (Strycharz et al., 2021). Users have experienced the practical and convenient benefits flowing from the collection of user data. Using the data to facilitate direct marketing for items or even personalized news feeds has saved users time and money (Strycharz et al., 2021). Industries that have built their business around selling this data or leveraging it to advertise will need to develop a way to survive without using cookies.

It should come as no surprise that as the internet moves to a cookie-less experience to help protect user data, there would be an interest in methods alternative to track and gathering user data. There is a conversation around several methods, including fingerprinting and DNS cache inspection.

Fingerprinting

Fingerprinting is a tracking method based on machine features (Klein & Pinkas, 2019). A profile of the device is created based on the characteristics of the machine used to visit a website. For example, this profile could include types of hardware components, operating system information, applications installed, or something as simple as fonts on the device. The idea is to create something similar to a biometric fingerprint, which would be easy to verify but challenging to forge for network-attached devices or systems (Bezawada et al., 2021). Using this unique fingerprint would allow for user tracking and data collection.

DNS Cache Inspection

DNS cache inspection uses the local device's stored or cached resolver data. A feature of DNS is to keep resolution information for frequently visited sites in a locally cached copy to help speed up the resolution process. This locally stored cache can be utilized to help track a user. To summarize the process, a code snippet must be activated from a website that intends to track a user. This snippet then accesses the local cache and creates a unique identifier for the user based on the stored resolver data; the identifier is also stored locally. As web browsing activity continues and sites are visited with tracking snippets, the unique identifier can be accessed, and data will be shared with the site that has been called (Klein & Pinkas, 2019).

Data Privacy Protection: The European Union versus the United States

Since the European Union's General Data Protection Regulation (GDPR) became effective in 2018, the websites of multinational companies now ask visitors to their web pages to accept their collection of cookies. Some sites will even go as far as not to allow a user to continue browsing unless they accept the cookie tracking. Most sites will allow a user to continue browsing but will dedicate an inconvenient portion of the page to the cookie collection notice and agreement. The GDPR is a broad and sweeping piece of legislation that puts user data at the center of its purpose and intent. (Zaeem & Barber, 2020). The law has multiple user data privacy mandates, and its reach is vast and spans international borders. (Zaeem & Barber, 2020).

In the United States, consumer data privacy has protection at the federal level and in some states within various sectors. Generally speaking, the federal government has placed data privacy under the umbrella of consumer protection. As such, the Federal Trade Commission (FTC) is responsible for enforcing laws designed to protect user data on the internet. The use of the internet evolved in different industries over the past two decades. Focusing on unfair trade practices, the FTC emerged as the primary agency for consumer data privacy enforcement in the mid to late 1990s (Solove, 2014).

No broad and sweeping federal law or regulation provides data privacy protection for consumers in the United States the way the GDPR does. Rather than one all-encompassing regulation or law addressing data protection, the United States has specialized sector-specific data privacy laws, none of which are regulated by a single federal administrative agency. In the US, data privacy laws such as the Children's Online Privacy Act, the Fair Credit Reporting Act, and the Gramm-Leach-Bliley Act are administered by different federal agencies and are part of entirely different pieces of legislation. The Gramm-Leach-Bliley Act requires institutions that offer financial services to the consuming public to maintain the security of user data up to specified standards and to disclose any consumer information sharing practices. Under the FTC Act, the Federal Trade Commission is authorized to investigate and impose penalties on companies that engage in unfair or deceptive practices that, among other things, compromise consumers' privacy (Federal Trade Commission Act, 1914).

Another example is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Family Educational Rights and Privacy Act of 1974 (FERPA). HIPAA requires covered entities— health care providers, health insurance providers, and their business associates— to protect patient health information through its Privacy, Security, and Enforcement subsections. The United States Department of Health and Human Services (HHS) investigates claims involving non-compliance with HIPAA and may impose financial penalties for violations of the law.

FERPA sets minimum standards for the protection of student education records. The records must be treated as confidential, and education institutions in the US are required to safeguard them from disclosure without legal consent. While there is no private right of action allowed by HIPAA or FERPA, individuals whose information is improperly disclosed may file complaints with the Department of Health and Human Services or the Family Policy Compliance Office of the US Department of Education, respectively. In cases where a statute does not provide a private right of action against an offending entity, individuals may seek personal recourse under their state's privacy statutes or common law precedents establishing individual recovery for invasions of privacy.

In 2012, the FTC settled a consumer protection case against Google for USD 22.5 million for allegedly failing to adequately disclose its cookie tracking habits on Safari users (Fair, 2012). A class of users also filed a class action lawsuit against Google for illegal cookie tracking practices. (In re Google Inc., 2015). The class claimed their user settings were set to block cookie tracking, yet Google still used cookies to track their browsing sessions (In re Google Inc., 2015).

What Data is Considered Worthy of Privacy Protection?

The regard for data privacy varies between the US and the EU. In the US, many individuals' expectations regarding online privacy seem to depend on the type of user data being compromised. For instance, in the US, many view minor invasions of their consumer privacy online as a cost of doing business or for the convenience of shopping online. On the other hand, most Americans will view a breach of their personal health information as an unacceptable violation of their privacy. The EU's Charter of Fundamental Rights states that everyone is entitled to respect their confidential information and that such information should be protected. While the US Constitution does protect privacy rights, it only protects them from government intrusion. Unlike the negative

rights that the US Constitution provides, the European Charter of Fundamental Rights provides for the positive rights, e.g., healthcare, education, and privacy, that citizens in the EU are entitled to be afforded by the state (Jones & Kaminski, 2020).

The EU has a much simpler approach to addressing the issue of data privacy than the US. The General Data Privacy Regulation (GDPR) is a data protection regulation that became effective in May of 2018 in the EU. The requirements of the GDPR apply to companies that collect and process information belonging to EU citizens (Zaeem & Barber, 2020). Any multinational organization, regardless of where it is based, must adhere to the requirements of the GDPR if they do business or market to citizens of the EU and collect and process their personal information. Additionally, the GDPR outlines a fine structure for violations which can be up to 20 million Euros (Gruschka et al., 2018).

Fragmented Privacy Legislation in the United States at the Individual State Level

Several individual states have chosen to enact data privacy protection regulatory schemes. The states that have passed or introduced comprehensive data privacy legislation have attempted to model their laws after the GDPR. Of the few comprehensive privacy laws passed at the state level, only California's law allows individuals a private cause of action for data privacy violations. California, Virginia, Colorado, and Utah have all passed comprehensive privacy legislation, with 13 states that have proposed legislation that remains unenacted (Lively, 2022).

California is a state that has heavily regulated in this arena, likely because of all the technology companies that call California home, including Apple, Google, and Facebook. In 2018 when California enacted the California Consumer Privacy Act (CCPA), it significantly expanded consumer notice requirements, rights, and the ability to opt-out and delete one’s user data. It also provided consumers with a right to non-discrimination, and it created an ability for the state to impose fines for violating the demands of the legislation. Fines can range from $2,500 to $7,500, depending upon whether the violation was intentional. (California Consumer Privacy Act § 1798.155, 2018). Additionally, the legislation allows consumers to file civil suits against companies for violating the law (California Consumer Privacy Act § 1798.150, 2018).

Currently, comprehensive privacy legislation only exists at the state level in the US. If this continues, "potentially conflicting privacy laws . . . will not only confuse consumers but [will] also impose high costs on organizations, as they will have to comply with differing laws from multiple states" (Castro, 2022, para. 5). A federal comprehensive data privacy law in the US would establish consistent and clear guidelines for the various data-driven businesses conducting business within its borders and beyond. Clear and consistent guidelines would allow companies to properly allocate their risk and ensure compliance with the law. Arguably, comprehensive federal data privacy legislation in the US should preempt state data privacy laws and not include a provision giving individuals the right to bring litigation to avoid opening "a floodgate of expensive, and unnecessary, lawsuits against organizations subject to the new law" (Castro, 2022, para. 7). Comprehensive legislation in the US similar to the GDPR, that sufficiently fines or otherwise penalizes companies for data privacy violations should adequately protect individuals without the need to give people the right to individual litigation.

Conclusion

Data privacy is regarded and handled in vastly different ways by the EU and the United States. The EU has created a robust and targeted approach to how websites can collect and utilize data. The United States has taken a segmented approach that combines multiple data laws limiting the overall control a user has over their data. With end users' growing social and political concerns regarding data privacy, the technical methods for creating a worldwide web that meets these demands have begun to take form. Technology companies like Google have made significant investments to create a universal technical standard that eliminates cookies with the intent to give users more privacy.

While eliminating cookies from the world wide web sounds like a solution that could meet the needs of all the parties involved, eliminating cookies from the world wide web could have potential downsides and create limitations. It will change the user experience by eliminating the personalization they have grown accustomed to. It will also reduce the ability of marketing firms to target advertising to users, which adds value to both the advertiser and the user. Because there is value in the collected user data for both the user and marketer, two potential workarounds are fingerprinting and DNS cache inspection. These methods would still allow for limited tracking and gathering of user data.

Future research will focus on whether new data collection methods will adequately fall within the bounds of evolving privacy regulations. As fingerprinting requires collecting information about a machine used to visit websites, will this scan and data collection of a user's machine comply with evolving laws? In the future, will DNS cache inspection require consent to initiate code from a website that would scan and collect resolver records? Marketers will likely face increasing challenges surrounding balancing their tracking activities to further their business objectives while providing an enhanced user experience with regulatory compliance, users' demands, and increased expectations for privacy.

References

Beigi, G., Guo, R., Nou, A., Zhang, Y., & Liu, H. (2018). Protecting User Privacy: An Approach for Untraceable Web Browsing History and Unambiguous User Profiles.

Bezawada, B., Ray, I., & Ray, I. (2021). Behavioral fingerprinting of Internet-of-Things devices. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 11(1), e1337.

California Consumer Privacy Act, Cal. Civ. Code § 1798.150 (2018).

California Consumer Privacy Act, Cal. Civ. Code § 1798.155 (2018).

Castro, D., Dascoli, L., & Diebold, G. (2022). The Looming Cost of a Patchwork of State Privacy Laws. Information Technology and Innovation Foundation.

Fair, L. (2012, August 9). Milking cookies: The FTC's $22.5 million settlement with Google. Federal Trade Commission. Retrieved November 20, 2021, from https://www.ftc.gov/news-events/blogs/business-blog/2012/08/milking-cookies-ftcs-225-million-settlement-google.

Federal Trade Commission Act, 15 USC §§ 41-58 (1914).

Gruschka, N., Mavroeidis, V., Vishi, K., & Jensen, M. (2018). Privacy Issues and Data Protection in Big Data: A Case Study Analysis under GDPR. *2018 IEEE International Conference on Big Data (Big Data)*, 5027-5033.

Rudo, H. P., & Reagan, A. (2021). The global landscape of data privacy: Important points about new laws in three key jurisdictions. *Practical Compliance - DLA Piper*

Improving Web Advertising Business Group. (2020, August 26). Https://Www.W3.Org/Community/Web-Adv/. https://www.w3.org/community/web-adv/

In re Google Inc., 806 F.3d 125 (2015). https://www.leagle.com/decision/infco20151110158

Jones, M. L., & Kaminski, M. E. (2020). An American's Guide to the GDPR. Dev. L. Rev., 98, 93.

Klein, A., & Pinkas, B. (2019, February). DNS Cache-Based User Tracking. In NDSS.

Klosowski, T. (2021, September 8). The State of Consumer Data Privacy Laws in the US (And Why It Matters). Wirecutter: Reviews for the Real World. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Lively, T. K. (2022, April 7). US State Privacy Legislation Tracker. Retrieved from https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

Schuh, J. (2019, August 22). Building a more private web. Google. https://www.blog.google/products/chrome/building-a-more-private-web/

Schuh, J. (2020, January 14). *Building a more private web: A path towards making third party cookies obsolete*. Chromium Blog. Retrieved June 25, 2022, from https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

Schuh, J. (2021, January 25). Privacy Sandbox in 2021: Testing a more private web. Chromium Blog. https://blog.chromium.org/2021/01/privacy-sandbox-in-2021.html

Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. Columbia Law Review, 114(3), 583-676.

Strycharz, J., Smit, E., Helberger, N., & van Noort, G. (2021). No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. Computers in Human Behavior, 120, 106750.

World Wide Web Consortium. (n.d.). *About W3C*. W3C. Retrieved from https://www.w3.org/Consortium/

Zaeem, R. N., & Barber, K. S. (2020). The effect of the GDPR on privacy policies: Recent progress and future promise. ACM Transactions on Management Information Systems (TMIS), 12(1), 1-20.