Framing Public Policy for Internet Data Privacy

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Saiteja Bevara
Spring, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature  Date __5/6/2021__
Saiteja Bevara

Approved ___  _____ Date __5/4/2021____
Hannah Rogers, Department of Engineering and Society

Abstract

The amount of data on the internet is increasing, and questions about collection and processing of this data have raised concerns about internet data privacy and protecting the rights of individuals. These concerns have led to the introduction of some user-centric legislation such as the GDPR. However, internet data as a technology is shaped by other groups in addition to individuals, namely companies and governments, and there is still a lack of comprehensive federal privacy policy in the United States.

This paper aims to analyze how internet data is interpreted and shaped by various social groups in individuals, companies, and governments through the Social Construction of Technology framework. Then, through the use of policy analysis of the GDPR, the paper evaluates the current policy landscape to determine how existing policy conforms to the values of these social groups. Findings show that although the GDPR does provide more theoretical privacy rights to individuals, there are still flaws in the practical implementation of the regulation. There is also a lack of clarity on issues of national security and incompatibilities or burdens in practical implementation of stricter regulations for companies. Policy will likely continue to be individual privacy-focused short-term, but will evolve as the downsides to GDPR-like regulation become apparent in the future.

Framing Public Policy for Internet Data Privacy

Introduction

As of 2018, an estimated 2.5 quintillion bytes of data were generated each day across the Internet. The amount of data generated between 2016 and 2018 alone accounted for 90 percent of all data in the world (Marr, 2018). The volume of internet data is increasing, and controlling access to this information and its potential uses is a growing concern. This concern was in the global spotlight when Facebook admitted that political consulting firm Cambridge Analytica had secretly collected the information of nearly 87 million users of its platform, using this information to influence voters during the 2016 presidential election (Kang & Frenkel, 2018). In the more recent context of the COVID-19 pandemic, vast amounts of user data became the foundation of technologies that allowed researchers to track the spread of the virus, raising questions about the value of data and its potential to benefit the common welfare (Fahey & Heno, 2020).

Protecting this rapidly growing user data is at the heart of internet data privacy. Privacy at a high level can be described as the "right to be left alone" (Warren & Brandeis, 1890). Internet data privacy, more specifically, can be categorized as a subset of information privacy, which is defined as the ability of an individual to control their personal information and how it is communicated with others (Hong & Thong, 2013, p.276). The issue of how to protect internet data privacy and problems with current privacy standards has become more important recently within the context of the amount of data being generated and the revelations of its misuse, particularly the Cambridge Analytica scandal. These concerns have led to calls for stricter data protection and internet data privacy legislation.

In response, legislation has been introduced abroad such as the European Union's (EU) General Data Protection Regulation (GDPR) which aims to protect individual privacy rights. In the US, legislation for this issue is only targeted at specific industries, such as the Health Insurance Portability and Accountability Act (HIPAA) for health-related information or the Gramm-Leach-Bliley Act that applies to financial institution data. Policy also has been introduced at the state level including the California Consumer Privacy Act (CCPA). The plethora of industry and state-specific pieces of legislation shows a lack of cohesive and comprehensive policy standards. There are some arguments that these more specific policies are beneficial, as they allow for more targeted regulation (Phillips, 2018). However, such specific legislation can ignore certain types of information not under its scope, or not cover innovative technologies which are yet to come. A greater number of privacy laws also places a greater burden on companies that must comply with varying privacy standards. Therefore, there is a need for policy reform in the US at the federal level, as current federal data privacy legislation is segmented, non-comprehensive, and narrow in scope (Mulligan, Freeman, & Linebaugh, 2019).

While implementing data privacy legislation may seem trivial from the perspective of simply aiming to protect individual user privacy, policymakers must take into consideration other factors. Interactions with internet data reveal other actors besides individuals, namely companies and governments, whose interests and values do not necessarily align with those of individuals or with each other. Individuals are primarily interested in protecting their data for the sake of personal autonomy. Companies focus on gathering data due to its value for their business models or to assist in developing other technologies. For governments, internet data is viewed as a tool to identify national security threats.

With their different interpretations of internet data, the approaches and perspectives on internet data privacy differ for each of these groups with individuals generally favoring stricter privacy standards and companies and governments preferring more access to data. Thus, the issue of crafting public policy to address internet data privacy is complex and requires further analysis, as it must be understood from the perspectives of all stakeholders. This paper will investigate the issue of framing data privacy policy around the interests of individuals, companies, and governments while specifically analyzing the GDPR from this viewpoint.

Social Construction of Internet Data

The human and social dimensions of internet data reveal the concerns of several relevant social groups, including individuals, businesses, and governments, who interact with internet data in different manners. The Social Construction of Technology framework is beneficial in analyzing how these various social groups interpret and shape internet data technologies. This framework focuses on the *interpretive flexibility* afforded to technologies as they develop. Social groups interacting with any given technology have a certain set of values and interests that will dictate the perspective and meaning given to that technology by that group. Based on these interpretations, problems can be identified that each group hopes to address relating to the technology. Solutions and alternate designs result from these various problems, building a *multi-directional model* of artifacts, social groups, problems, and solutions that display the evolution of technologies and considerations in its development (Pinch & Bijker, 1984). Analyzing internet data as a system from the perspective of relevant social groups of individuals, companies, and governments can help in framing privacy policy appropriately.

Individuals, in this context representing regular users of communication services, social platforms, or other internet-enabled devices, use technologies and social platforms on a near-daily basis, and for them internet data presents a major privacy concern at a personal level. They are considered a relevant social group in their interactions with internet data as it is their own data which is being collected and processed. For these users, individual human rights are the foundation for values they look to uphold, and data privacy directly relates to this interest. One such right is the human "right to privacy", recognized constitutionally in many countries and even in the United Nations Universal Declaration of Human Rights as a fundamental right for all humans. But beyond this concrete right to privacy, privacy itself is also directly related to individual autonomy (Bernal, 2014). Privacy and autonomy effectively enable human rights and civil liberties such as freedom of expression, religion, and speech, which highlights how the impacts of privacy transcend online activities and impact real-world experiences. As Bernal (2014) mentions, one particular example of how privacy protects autonomy is the use of data to tailor content for individuals, which directly influences their choices on the internet and removes a layer of freedom from their daily lives. It also gives more opportunity for behavior such as price discrimination or other demographic based predatory practices from data collectors and processors. The internet has become an intrinsic part of everyday life for individuals, and protecting their internet data privacy is critical in defending their basic human rights (Bernal, 2014).

Companies are another social group that shape data privacy systems, and represent those who control the major platforms which ultimately collect and process user data. In most cases, the collection of information and data is directly relevant to their business model. Corporations aim to use user data to drive targeted content delivery such as through marketing and advertising,

improve their products and performance through data metrics, or sell the data to other companies. In many cases, internet data is what enables companies to provide services to users for free as user data becomes the product. This leads to questions over the monetary value of internet data. In a single quarter of 2019, Google and Facebook earned $32.6 billion and $16.6 billion in advertising, respectively, emphasizing how companies are able to benefit from data (Baca, 2019). The World Economic Forum even signified personal data as an asset class in 2011, and went as far as to envision a future where personal data would be equivalent to a form of currency (*Personal Data: The Emergence of a New Asset Class*, 2011).

Companies may also use internet data for tasks which benefit the general public, such as during the COVID-19 pandemic to track the spread of the virus or to better understand societal inequalities which contribute to higher rates of sickness in communities of color (Brill, 2020). Data is also being used commonly as the backbone for complex algorithms, such as in machine learning to train models for purposes such as disease diagnostics (Shen et al., 2019). In these scenarios, collecting a large amount of data is critical in order to achieve desired efficiencies or accuracy. This has been followed by the growth of fields such as Big Data, Cloud Computing, and Artificial Intelligence which are all characterized by or can involve large degrees of data collection and processing. Thus, an ability to maintain economic incentives and pursue specific data related tasks, albeit beneficial or harmful, remains the current focus for companies in collecting and processing internet data.

Finally, governments interact with internet data largely for national security. The internet and social media platforms enable criminals and harmful third parties to communicate. Internet data provides a source for governments to surveil and track security threats. From a regulatory perspective, it can be said that the interests of individual privacy disagree with national security

concerns. There is a concern that protecting the absolute right to privacy for all individuals may impede the ambitions of governmental and other security organizations from comprehensively tracking threats to national security and welfare. This was apparent in one specific instance following the 2015 Paris attacks, as the Obama administration designated encryption technologies that obfuscated user data as platforms for adversaries to freely communicate (Sanger & Perlroth, 2015). Another example, at a much larger scale, was the PRISM program, which collected information about individuals for the purpose of surveillance at the expense of individual privacy. Governments thus view internet data as a significant source in identifying security threats, and data privacy becomes a hindrance to these tasks.

In the early stages of the internet, internet data may have been limited to the data that was voluntarily submitted on websites by users. Today, internet data comes from an unprecedented number of sources in unexpected forms, including regular communication such as texts and emails and extending to the complex activity and behavior patterns of users that is tracked over multiple platforms and technologies. Overall, internet data has stabilized today as a valuable commodity, whether it is for the purposes of privacy, business, or security. With a shift towards prioritizing the issues presented from the individuals' point of view due to recent data breaches and infringement of privacy rights, policy will no doubt be a major factor that will shape internet data technologies and practices in the future. Policy makers must, therefore, keep in mind the social construction of internet data and the values of each of the relevant social groups when regulating data practices.

Current Policy Landscape and GDPR

A report by the Congressional Research Service (2019) analyzed the landscape of current privacy legislation within the United States (Mulligan, Freeman, & Linebaugh, 2019). Findings showed a "patchwork" of individual legislation that was technical and complex, and was targeted at specific fields and industries or specific categories of data. These industry specific acts demonstrate a lack of comprehensive legislation at the federal level (Mulligan, Freeman, & Linebaugh, 2019). This paper hopes to understand how to appropriately frame internet data privacy legislation.

Analyzing privacy regulations which have already been implemented can provide insight into potential frameworks which the United States can incorporate into federal privacy legislation. These regulations can also be analyzed from the perspective of individuals, companies, and governments to identify how it affords value to the interests of these groups. This paper will focus on the GDPR as it is the most comprehensive and established data protection legislation that currently exists.

GDPR

The GDPR was introduced as a revolutionary privacy framework. It was based on the idea of privacy as a fundamental human right, defending their right to protection of personal data (Goddard, 2017). Personal data as defined by the GDPR covers information relating to any identifiable individual. The core privacy principles are as follows, where each principle relates to how personal data should be handled:

- "Lawfulness, fairness, and transparency": data should be processed in a lawful and transparent manner
- "Purpose limitation": data should be processed and collected only with a specific purpose unless it relates to the public interest or scientific or historical research

- "Data minimization": only necessary data is to be collected
- "Accuracy": reasonable steps should be taken to maintain personal data is accurate and up to date
- "Storage limitation": data which allows identification should only be kept for as long as necessary to achieve original purpose
- "Integrity and confidentiality": data should be collected and processed in manners that guarantee its security
- "Accountability": Data controllers are responsible for complying with the GDPR

The GDPR also requires a legal basis for the processing of data, which can manifest in six possible forms: consent, performance of contract, compliance with legal obligations, protect vital interests of subject, public interest, or other "legitimate interests" of the companies that do not infringe on the personal rights of the subjects. Consent is also demanded to be freely given, specific, informed, and unambiguous. Moreover, the GDPR provides users with explicit rights, such as the right to be informed, right of access (to their personal information), right to rectification (correct inaccurate information), right to erasure (or right to be forgotten), right to restrict processing, right to data portability, right to object (to processing of their data), and rights specific to automated decision making and profiling.

Analysis of GDPR

The GDPR has been considered one of the most privacy-first and user-centric policies introduced. Analyzing the regulation from the perspectives of all relevant stakeholders reveals the affordances to each social groups' values with regards to internet data. In doing so, the *interpretive flexibility* aspect of the SCOT framework is being applied to understand how each distinct group within the stakeholders interprets internet data privacy as it appears in the GDPR.

From an individual's standpoint, it is clear that the explicit rules and restrictions placed on the collection and processing of user information, and the agency of users to be forgotten and for data portability amongst other rights places their values of a human right to privacy as a major priority. Therefore, the GDPR overall is a net positive for individuals in protecting their human rights. However, some flaws exist in protecting individual privacy, as highlighted by van Ooijen & Vrabec (2019) who analyze how the GDPR influences individual control over data. For one, the GDPR does give individuals the right to information on how their data is being used, which directly influences their control over their data privacy. However, van Ooijen and Vrabec found that there are no specifics on informational complexity requirements, which means companies are able to provide confusing and complex data use policies with low readability for users. This highlights how although the GDPR does theoretically provide individuals with more agency in their privacy, in reality the privacy practices of individuals can be limited. Moreover, in the age of artificial intelligence and automated data processing, some algorithms are simply hard to convey to users, which means individuals may not be able to get sufficient information on how their data is being used. The GDPR has no information on what to do in scenarios like this, showcasing another weakness in its adaptation to newer or complex technologies when protecting individual privacy.

In yet another study, the theoretical advantages the GDPR provides to individuals was again found to be lacking in real world scenarios. The language companies used was found to be vague, default settings on sites were found to not be privacy-first, and the right to request information was found to be inadequately handled (Jakobi et. Al., 2020). In essence, it is clear the GDPR was not doing enough to promote individual privacy as it may seem at first glance. However, the stipulations that data collection requires informed consent and increases

restrictions on when to process or store data (only with a specific purpose) strengthen individual privacy concerns, so the GDPR can still be considered helpful to individual privacy overall (Jakobi et. Al., 2020).

From the perspective of companies, their lobbying efforts benefited them by continuing to allow them to process non-sensitive information for business purposes through the "legitimate interest" clause (Davies, 2016). Thus, there are still numerous avenues through which data processing can occur, especially with consent given under the conditions specified by the GDPR, which means there is not a complete overhaul for companies which rely on data for their business models. However, it is clear that the drastic changes which are required of this policy do place a burden on companies who must alter their technologies to adhere to new standards.

Estimates from 2017 indicated Global Fortune 500 companies would spend $7.8 billion for GDPR compliance, a considerable amount that displays the difficult nature of complying with new privacy standards (McQuinn & Castro, 2019). Larger implications are that provisions similar to GDPR standards in the United States would cost the entire US economy $122 billion per year, another hesitation in implementing GDPR-like privacy regulations in the US (McQuinn & Castro, 2019). Furthermore, for companies who collect data to tailor user experience, especially with the use of devices that collect data in non-explicit manners or IOT devices, consent may be harder to solicit and thus can impede these operations (Lee, Cha, & Kim, 2019). Therefore, even though the GDPR is correct in requiring consent in these forms of data collection to protect privacy, it presents another obstacle that companies must go out of their way to solve which may stifle innovation. The burden of changes due to the GDPR was best reflected in a survey conducted by Gartner in 2019, which revealed executives surveyed considered "accelerating privacy regulations" as the top emerging risk, requiring more infrastructure for IT,

legal, and information security divisions (*Personal Data: The Emergence of a New Asset Class*, 2011). There is also evidence that short-term impacts of GDPR included lower venture capital investments in EU firms, especially for data-related or consumer facing businesses, which means the GDPR directly hurt companies' financials (Jia, Jin, & Wagman, 2021).

Strict privacy regulations such as GDPR can also benefit large companies at the expense of smaller companies, stifle innovation, and bar new market entrants. Larger companies have more resources and take advantage of economies of scale that allow them to bear compliance costs easier (Phillips, 2018). From a competitive standpoint, the consent requirement from the GDPR helps larger companies due to the "brand effect" of them being more recognizable, which was evident in Europe as digital advertising companies decided to stop operating in Europe solely due to consent requirements (Phillips, 2018). According to Johnson et. Al. (2019), regulations may have made it easier for larger technology firms and vendors to acquire consent or adhere to restrictions compared to smaller vendors. Therefore, there was an increase in market concentration that coincided with more data privacy, which increased anti-competitiveness in the region (Johnson et. Al., 2019). The GDPR had, by establishing stricter policy, in effect hurt industries by making them less competitive. In a more direct sense, companies' ecommerce revenues also fell by 13.3% and web traffic decreased by 11.7%, representing significant losses for ecommerce companies due to GDPR regulation (Goldberg, Johnson, & Shriver, 2021). Thus, companies, especially smaller ones, were severely hurt by GDPR privacy regulations. Excluding competitors can increase market concentration and give larger companies control over certain industries or allow them to raise prices, which can even hurt end users (Brill, 2019). Relating to innovation, the GDPR has many consequences for innovative and developing technologies that rely on data, such as Artificial Intelligence and Big Data technologies. Companies also lose the

ability to experiment with data or reuse existing data for new purposes due to the purpose specification and data minimization requirements of the GDPR, which indicate companies must have a clear purpose for using data and must only collect and use data that is necessary for this purpose (Chivot & Castro, 2019).

For governments, Article 23 allows individual member states to restrict the applications of the law, and therefore the rights of individuals, for purposes of "national security, defense, public security...or 'other important objectives of general public interests'" (Davies, 2016). This means member states of the EU have the ability to bypass restrictions for their own objectives. They have flexibility in collecting and processing individuals' data provided they prove their purpose and are using the data in a lawful manner to protect the fundamental rights and freedom of individuals (Wagner & Benecke, 2016). However, this lack of exact specifications still does not clarify the line between privacy and security. In the EU, the responsibility to ensure this balance rests on data protection authorities such as European Data Protection Supervisor who must cooperate with governmental institutions to safeguard privacy while maintaining security ("Data Protection | European Data Protection Supervisor," n.d.).

Crafting Privacy Policy for Individuals, Companies, and Governments

The disjointed data privacy policy landscape requires discussion on how to frame comprehensive federal legislation in the United States. Analyzing existing legislation, the GDPR presents ideas which are good baselines for future policy implementation, especially considering the context of the legislation being the first of its kind. The regulation reveals certain philosophies that are beneficial to the problem-solution models which the social groups that

shape internet data define. However, there are also clear flaws in its design which require consideration when moving forward.

For individuals, the explicit rights which are outlined are a step in the right direction towards protecting user data. They require consent under strict conditions and provide key principles such as the right to be informed, the right to be forgotten, and the right to portability among others. United States legislation should use the principles of privacy from the GDPR as the foundation for individual privacy at a federal level, especially with the enumerated rights that give baseline values to the overarching "right to privacy". However, although in theory the rights which are afforded to individuals are present, reality indicates that a lack of specificity hurts individuals. Methodologies which companies use to adhere to requirements can vary, such as the use of complicated data use policies that solicit consent. Therefore, requiring consent is not enough, but rather more guidance is needed on how companies can appropriately get consent from individuals through clear and understandable policies and actions. Policy makers should look to engage in dialogue with individuals to determine how flexibility in implementation or interpretation of regulations can hinder the expression of privacy rights, whether that requires more specificity or collaboration between individuals and companies. One solution could be to have industry agencies take charge in establishing guidelines for how certain types of data collection can be better understood and acted on by individuals. Although this is similar to the structure of current US legislation with its industry specificity, these would instead simply be guidelines that data collectors could use to better communicate with individuals and allow them to practically utilize their rights, all under a preemptive and comprehensive federal data regulation.

For companies, the GDPR does present a large hurdle. In the name of improving individual user privacy, there are stricter regulations which firms must adhere to. Much discussion has occurred on the downsides of stricter policy regulation for companies and their values with regards to internet data. For example, evidence has shown that GDPR can lead to anti-competitiveness or stifle innovation, and increase costs due to compliance and infrastructure. Therefore, US privacy legislation should ensure that compliance is not overly arduous, especially for smaller or newer companies or those in fields which are unequivocally devastated by data restrictions. Some might argue that companies should be able to bear costs for the purposes of privacy. While this is true to some degree, these regulations and costs also hurt the end user, through less access to free services, increase in prices, or worse user experience such as less personalized content or worse products from companies with smaller budgets or a monopolized market that leaves little motivation for improvement. In the name of privacy, it is understandable to sacrifice these rights, but the hidden costs of privacy must be communicated to individuals. Future legislation or frameworks for privacy must find a way to strike a balance between privacy and competition, or more broadly protect the interests of both individuals and companies to benefit privacy and economic prosperity.

Moreover, national security concerns should remain an important priority. The GDPR has a decent amount of ambiguity and provides individual countries broader powers to implement national security guidelines for data use. This flexibility means responsibility is placed on cooperation between data protection authorities and security institutions themselves to regulate the use of personal information for security concerns. In the United States, the option to delegate privacy policy implementations to individual states is not as feasible as delegating it to member countries of the EU, where regulatory agencies have more capabilities to implement and enforce

policy decisions relating to privacy. Therefore, there must be strict guidelines for what exact purposes data can be collected and used for, but nevertheless there must be clauses which afford government agencies the ability to bypass certain data privacy laws in the name of common good, as the GDPR has done. Nonetheless, finding the right balance between protecting individual rights and defending the use of data for national security does require a more focused effort for analysis, especially from an ethical standpoint of protecting individual rights instead of the common good.

Conclusion

Internet data is growing at a rapid rate, and controlling access to it is a major concern. Individuals, companies, and governments have forced the need for policy makers to frame privacy regulation to prioritize individual autonomy, national security, and economic growth because major social groups which shape internet data have conflicting values for how privacy should be approached. Current comprehensive policy standards such as the GDPR provide affordances to the values of these social groups, but as analyzed in this paper there exist flaws which must be corrected when framing similar policy in the United States. To protect the right to privacy and autonomy of individuals, the practical implementation of privacy rights must be better understood to ensure individuals are able to properly exercise their agency to protect their data. For companies and the overall economy, privacy regulations must be introduced without damaging business, asymmetrically hurting smaller companies, harming competitiveness, or stifling innovation. In the name of promoting national security, there must be open dialogue between individuals and governments on how data is being used to protect their well-being.

Moving forward, policy will most likely continue to be user-focused and primarily work to increase the privacy and agency of individuals, at least in the short-term following events such as the Cambridge Analytica scandal that have put the public on alert regarding the use of their data. In the US, privacy regulation will likely take similar form to the GDPR without addressing many of the flaws which were outlined in this paper, simply because the current focus will be on individual privacy rather than the interests of all stakeholders. Legislation will also be introduced relatively soon, as Congress has been deliberating on stringent privacy regulation for the past few years and comprehensive privacy legislation has bipartisan support.

However, the consequences of not framing privacy policy around the interests of all groups, or not understanding how the implementation of these standards would practically work towards these interests, will reveal themselves as they are beginning to for the GDPR. Individuals will then vocalize their inability to properly understand or employ their privacy rights, resulting in more specific legislation which can be implemented to impact individuals more realistically. The effects of burdensome regulation on companies and the adverse effects of strict privacy regulations on the economy and industries will take shape, resulting in some privacy standards being relaxed for the benefit of both users and companies. Depending on public perception of national security threats at any given time, privacy exceptions for security agencies will probably change course multiple times and never reach a concrete conclusion.

Future technologies and developments in the data industry will also continue to shape data privacy. New methods of gathering information and newer methods of utilizing this data means data privacy understandings and interpretations will change for relevant social groups. As the Artificial Intelligence space grows, for example, users might see these technologies as precursors to change their interpretations of internet data from a primarily privacy concern to a

necessary sacrifice to enjoy the benefits of such technologies. Innovative technologies such as Internet-of-Things (IOT) devices and new sensors might also present a hurdle for privacy regulators who must alter their definitions of consent which is harder to solicit for these new systems than for other technologies.

Additionally, this paper only focused on the GDPR to analyze how policy can be beneficial or harmful for relevant social groups. Future work could analyze other policies such as the CCPA or even industry specific acts like HIPAA, to gain insight into other possible policy frameworks. Moreover, this research is limited in its scope of only considering three major social groups, and even then, only considering their most important interests. The ethical considerations of privacy were also not discussed, but there are many perspectives on how ethical frameworks can apply to data privacy such as elements of common good or normative ethics. These ethical lenses can influence interpretations of how data privacy should be approached that can be investigated in future work.

References

Baca, M. C. (2019). What you do on the Internet is worth a lot. Exactly how much, nobody knows. *Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2019/10/14/what-you-do-internet-is-worth-lot-exactly-how-much-nobody-knows/

Bernal, P. (2014). *Internet Privacy Rights: Rights to Protect Autonomy*. Cambridge University Press.

Brill, J. (2020). Why privacy is essential to equitable recovery. Retrieved from Microsoft on the Issues website: https://blogs.microsoft.com/on-the-issues/2020/10/16/privacy-laws-open-data-economic-recovery/#_ednref1

Brill, J. (n.d.). The Intersection of Consumer Protection and Competition in the New World of Privacy. *Competition Policy International*, 18.

Chavot, E., & Castro, D. (2019). *The EU Needs to Reform the GDPR To Remain Competitive in the Algorithmic Economy*. 20.

Data Protection | European Data Protection Supervisor. (n.d.). Retrieved March 1, 2021, from European Data Protection Supervisor website: https://edps.europa.eu/data-protection_en

Davies, S. (2016). The Data Protection Regulation: A Triumph of Pragmatism over Principle Foreword. *European Data Protection Law Review (EDPL)*, *2*(3), 290–296.

Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. *International Journal of Information Management*, *55*, 102181. https://doi.org/10.1016/j.ijinfomgt.2020.102181

Gartner Survey Shows Accelerating Privacy Regulation Returns as the Top Emerging Risk Worrying Organizations in 1Q19. (2019, April 11). Retrieved March 1, 2021, from Gartner

website: https://www.gartner.com/en/newsroom/press-releases/2019-04-11-gartner-survey-shows-accelerating-privacy-regulation-returns-as-the-top-emerging-risk-worrying-organizations-in-1q19

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European Regulation that has a Global Impact. *International Journal of Market Research*, *59*(6), 703–705. https://doi.org/10.2501/IJMR-2017-050

Goldberg, S. G., Johnson, G. A., & Shriver, S. K. (n.d.). *REGULATING PRIVACY ONLINE: AN ECONOMIC EVALUATION OF THE GDPR*. 49.

Hong, W., & Thong, J. Y. L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, *37*(1). Retrieved from https://www.jstor.org/stable/43825946

Jakobi, T., von Grafenstein, M., Legner, C., Labadie, C., Mertens, P., Öksüz, A., & Stevens, G. (2020). The Role of IS in the Conflicting Interests Regarding GDPR. *Business & Information Systems Engineering*, *62*(3), 261–272. https://doi.org/10.1007/s12599-020-00633-4

Jia, J., Jin, G. Z., & Wagman, L. (2021). The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment. *Marketing Science*, mksc.2020.1271. https://doi.org/10.1287/mksc.2020.1271

Johnson, G. A., Shriver, S. K., & Goldberg, S. G. (2019). Privacy & Market Concentration: Intended & Unintended Consequences of the GDPR. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3477686

Kang, C., & Frenkel, S. (2018, April 4). Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users. *The New York Times*. Retrieved from https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html

Lee, G. Y., Cha, K. J., & Kim, H. J. (2019). Designing the GDPR Compliant Consent Procedure for Personal Information Collection in the IoT Environment. *2019 IEEE International Congress on Internet of Things (ICIOT)*, 79–81. https://doi.org/10.1109/ICIOT.2019.00025

Marr, B. (2018). How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. *Forbes*. Retrieved from https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#5ebb2e0060ba

McQuinn, A., & Castro, D. (2019). *The Costs of an Unnecessarily Stringent Federal Data Privacy Law*. Information Technology and Innovation Foundation. Retrieved from Information Technology and Innovation Foundation website: https://itif.org/publications/2019/08/05/costs-unnecessarily-stringent-federal-data-privacy-law

Mulligan, S. P., Freeman, W. C., & Linebaugh, C. D. (2019). *Data Protection Law: An Overview*. Congressional Research Service. Retrieved from Congressional Research Service website: https://fas.org/sgp/crs/misc/R45631.pdf

Personal Data: The Emergence of a New Asset Class. (2011, January). World Economic Forum.

Phillips, N. J. (2018, July 27). “Keep It: Maintaining Competition in the Privacy Debate". Retrieved from Internet Governance Forum USA website: https://www.ftc.gov/system/files/documents/public_statements/1395934/phillips_-_internet_governance_forum_7-27-18.pdf

Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other. *Social Studies of Science*, *14*(3).

Sanger, D. E., & Perlroth, N. (2015, November 24). Iranian Hackers Attack State Dept. Via Social Media Accounts. *The New York Times*. Retrieved from https://www.nytimes.com/2015/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html

Shen, J., Zhang, C. J. P., Jiang, B., Chen, J., Song, J., Liu, Z., … Ming, W.-K. (2019). Artificial Intelligence Versus Clinicians in Disease Diagnosis: Systematic Review. *JMIR Medical Informatics*, *7*(3). https://doi.org/10.2196/10010

van Ooijen, I., & Vrabec, H. U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, *42*(1), 91–107. https://doi.org/10.1007/s10603-018-9399-7

Wagner, J., & Benecke, A. (2016). National Legislation within the Framework of the GDPR. *European Data Protection Law Review (EDPL)*, *2*(3), 353–361.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160