Understanding the Reasons Why Consumers Are Concerned About Their Data Privacy and Security

Tristan Woodard
Major of Cybersecurity
CYSE250
Old Dominion University

Abstract

Data protection and regulation are a disjointed and often unregulated realm of action. Access to cyber related tech and in turn, cyberattacks, are only growing in number. These breaches and attacks have left consumers heavily concerned about their data and its security. Corporate actors in general tend to have the opposite concerns. If the goal is consumer data security and privacy, then the data shows that more government regulation, usually with large fines as a punishment, is the best result for societal welfare, despite the objections.

Key Words: Consumer Data, Privacy, Regulations, Data Protections.

Introduction

With Cyberspace becoming as integral to many human lives as the material world, and the Internet of Things (IoT) an increasingly large part of a consumer's life, more and more concerns are developing with how both traditional and cyberspace based companies are storing, utilizing, harvesting, and selling consumer data. These concerns span a wide spectrum, just as the spectrum of how consumer data is utilized is just as wide. Some companies base their entire business model and profits on the explicit harvesting and selling of consumer data, while some merely collect consumer data out of necessity and only store it in a limited capacity. This has led to cyberspace and regulation space some could think of as akin to the wild west. Many believe there are little to no regulations or security in the cyber-world for these companies, while many consumers go about their business indifferently, seemingly satisfied with the current regulation and consumer data protection

landscape. Mirroring this behavior, some policymakers likely believe the entire cyberspace industry is largely self-regulating, while many also are calling for more comprehensive intervention and control. With the problems and solutions only proliferating more every day, one must look at the entire landscape to truly understand how we can best help all parties involved, and eventually, create a culture of security. In the following I will detail the current data privacy landscape, outline the many concerns with the current data privacy landscape, delve into the current regulations' situation concerning the landscape, and identify the potential impasse between the concerns of consumers and the incentives of business.

Current Landscape

When it comes to the current consumer data privacy landscape, most would not describe it as ideal. Combined with the overall proliferation of cyber reliant technologies, has come a proliferation of cyberattacks and breaches. For instance, the rate of phishing attacks in 2018, was doubled when compared to 2017 (Luo & Choi, 2022). This rise of attacks has resulted in numerous large scale and massive scale breaches to occur to major industry players that have caused real world damage to consumers. An infamous breach occurred in 2011, when the consumer data of 77 Sony customers was compromised. Sony directly paid out $15 million as compensation, and millions more in refunds, and legal fees. Other examples include a breach for Yahoo, which exposed the information of 3 billion separate accounts, and the U.S. retailer Target, whose 2013 breach of over 100 million consumers saw their short term profits cut in half. To give context to how prevalent these breaches have become, in 2020 it was estimated that in the U.K., roughly half of all businesses had seen a breach of some kind within the last year, with the number ballooning to 75% for large businesses (Malan et al., 2020). Many of these breaches likely are not made easier or less damaging because of reliance or usage of IoT technology. In the U.K. for instance, it is predicted that there will be an increase of 150 million IoT devices by 2024. In addition, it is expected that IoT “things” (Not traditional computers or smartphones) are to grow to larger numbers than traditional computers and smartphones within the coming years. In addition, the growth of synergistic technologies, such as 5G, will increase the utilization and usage of IoT technologies. Despite these facts, around half of all companies globally cannot tell if their IoT devices have been compromised or not. Another compounding issue making IoT devices especially vulnerable, is that they often cannot (or are not) easily updated after purchase and implementation, making them exceptionally vulnerable. In addition, the types of attacks that can be performed

on IoT devices can be described as not particularly difficult for an attacker to commit. Overall, it seems that cyber based technology, and especially IoT technology are being used more and more, with no signs of slowing down. In tandem with this, cyber-attacks are becoming more common, with security measures not particularly keeping up with the ongoing security needs.

The Concerns

With the landscape mapped out, we can begin to understand and analyze the concerns parties may have with the current landscape of consumer data privacy protections. One large concern customers have been that errors could occur in the storage, analysis, or usage of customer data (Hemker et al. 2021). This seems to be quite a well-founded concern, as it seems that around 95% of security breaches are caused due to human error (Malan et al., 2020). In addition to ensuring that data is used and analyzed responsibly and correctly, businesses are also in charge of assuring no human error occurs that can completely compromise all the data still being held, in addition to any remnants of customer data left in code, databases, offsite storage, backup storage, etc. Another common concern is the secondary use of data. One may offer up some sort of data point in return for an expected result. For instance, one may let a business know which sorts of music or food they prefer in exchange for a recipe or music recommendation. However, nowadays, customers are concerned about the potential secondary usage of the data given up. That data could be analyzed for some other secondary use, or even sold to another agency or company to further a secondary goal elsewhere. Another common concern is the unauthorized access of data. Again, the full protection of customer data as long as it is available is a tough task. Making sure there are no points anywhere in the data life cycle for an unauthorized user to access it is something customers expect, but may not always get. Overall, customers also seem to be concerned in general about the unclear nature of what exactly is being collected about them, and why. As the number of devices grow, the number of databases grow, the number of attacks grow, and the amount of data grows, the average consumer is getting less and less able to understand the sheer scope of data collection and utilization. This leaves them left in the dark and concerned as their data is being analyzed constantly. For an example of potential corporate concerns about the data landscape, the reaction and concerns related to the implementation of the California Consumer Privacy Act (CCPA) could be analyzed (Baik

2020). One clear concern on the corporate side is that if there are regulations, they are often too broad or unclear in their definitions. Another concern the corporate side often has is with the potential small business impact if regulations were to change. Economic growth due to data collection is often stressed as important, and corporate voices have often stressed a need for an "opt-in" or "opt-out" option for certain regulation strategies, depending on the company and need.

Regulations

One word that could likely be used to describe the current consumer data protection landscape is fractured. Many different countries and multinational entities have implemented their own separate standards and guidelines, all with different approaches and scope. One of the largest blocs of consumers and a trendsetter in the field is the European Union (EU) with its comprehensive General Data Protection Regulation (GDPR) and Personal Data Protection Acts (Luo & Choi, 2022). Another innovator on this stage is the People's Republic of China (PRC) which set into effect new data regulations in 2019 that imposed harsh fines for those that did not adequately protect consumer data. Thailand is another country that has implemented similar protections on a national level. Another route taken by some countries can be to devolve the matter to lower levels of government. The United States (U.S.) has taken this path, with no significant national level measures in place. So far, very few states have taken up the task of implementing their own sets of regulations and protections, with the CCPA being a notable exception (Baik 2020). Other countries have allowed the industry and companies to self-regulate, instead implementing programs and attempting to help the process that way instead (Luo & Choi, 2022). The United Kingdom (U.K.) for instance, has spent the equivalent of over $100 million U.S. Dollars to implement research programs and nationwide initiatives. Australia similarly has spent upwards of the equivalent of $230 Million U.S. Dollars in cybersecurity investments of a similar nature. One common specific requirement from the more comprehensive schemes, such as the GDPR, is the explicit requirement of consent from the consumer if the business wishes to process and move around the consumer's data. Another common requirement present in some schemes, such as the CCPA, is that if consumers do exercise their right to decline the data tracking or use, they cannot be discriminated against with price changes, reduced quality of service, denial of service, and the like (Baik 2020).

The Impasse

With the landscape, the regulations, and the concerns in mind, one could likely start to see the underlying major impasse likely to be at play in causing many customer concerns in a lack of consumer data privacy. Corporate and business interests in general, seem to prefer a self-policing policy, with little, or ineffectual regulations, and wish to be able to collect, utilize, and sell data as they please (Baik 2020). Consumers, to put it shortly, prefer seemingly the opposite of all those things. On the corporate side, corporate interests seem to stress the need for less (or no) restrictions on consumer data use and harvesting, as to impose such restrictions would lead to negative economic outcomes and hampering innovation. In general, using the corporate voices present in the debates surrounding the development and enactment of the CCPA, corporate actors treat data privacy as a commodity. In this framework, consumers are a target demographic to be used for data extraction for profit's sake and less than human beings. In contrast, most consumers seem to view privacy as a human right or expectation instead of a commodity one can buy with enough capital. The shade of the merit of the innovation argument is present, even if the overall goals and framing of the argument doesn't quite line up with consumer interests. Great strides have seemingly been made in the technology of consumer choice and data analysis and acquisition. For instance, researchers in 2020 were able to utilize the YOLOv3 algorithm to detect humans combined with the Kalman Filter algorithm to track them, and were able to achieve results of 85% detection (Kajabad et al., 2020). In 2018 researchers were able to utilize models and eye-tracking technology to determine that health claims outperform nutritional claims when it comes to consumer attention (Ballco et al., 2019). In particular, they were able to find dairy products received the largest boost, particularly when promoting a health claim related to cardiovascular health. These types of data innovations and studies do lend some nature of credence to the claims that consumer data can be informative and bring wellness to consumer lives. However, despite the real innovations in many technological aspects, the corporate actors tying their concerns to the real innovation bandwagon may be suspect in its veracity (Baik 2020). Innovation can often mean a multitude of smaller things. It can mean both product innovation and process innovation. Most often, though, innovation seems to mean some sort of change. This commonly accepted view of innovation stands in stark contrast to the way innovation is used and asserted by the various corporate interests present in the case study of the development of the CCPA. Corporate speakers often stressed that consumer data harvesting and utilization was

necessary in order to innovate. This frames consumer's expectations of security and privacy as being against innovation. In general though, it seems that often corporate interests are using the term "innovation", with its numerous positive correlation and connotations, as a way to say "absence of regulatory constraint". Innovation and security are often framed as trade-offs in this lens, as if when you turn the slider up on one, the other falls in response. Incidentally, this lens seems to turn the way innovation is used by corporate interests into an antonym of how innovation is in actuality. When used, it is used to attempt to maintain the status quo of a lack of regulation, privacy, and customer control, while an innovative position would be one that seeks change and improvement. This usage is akin to a motte-and-bailey fallacy. In this case, the "motte" is the usage of innovation that is closer to reality, and takes its connotations of improvement and technological advancement with it. The "bailey" then is the way innovation is used, often being a synonym for "lack of regulation". When challenged, corporate interests can retreat to the motte, and defend that position. The position of technological innovation and progress is hard to argue with, and it can often frame opponents as irrational and incorrect. When on the attack, however, the actor can reside in the bailey, using the much more difficult to defend definition as a tool to attack certain arguments and positions with their real concerns, only bothering to ever defend the much more easily defendable position. When viewing if these self-regulation schemes work, there are very few promising signs or data points that it seemingly does. In 2014 the FTC made efforts to spur more regulations and controls on data brokers, mostly on account of self-regulating monitoring and enforcement being perceived as a failure (Listoken 2017). When viewing other fields apart from cyber-related fields, at best the results of self-regulation seemed to be "mixed". Data and cyber related fields are unique, however, so even if other fields saw success, it may not necessarily translate. Overall, it has been shown that government penalty schemes and regulations, in contrast to self-regulation schemes, will always benefit suppliers and consumers, while hurting the e-retailer (Luo & Choi, 2022). When these regulations are designed to benefit consumers, these schemes have been analytically proven to benefit the general social welfare of a society. Heavy fines seem to be the optimal punishment for breaches in regulation. In select cases where fines are not beneficial, it is recommended that instead the government should encourage or direct certain industries to create logistical and strategic alliances with suppliers and business partners to increase security and trust.

Conclusions

In conclusion, the current cyber landscape is an ever-growing and expanding landscape with more room for breaches and human error, especially considering expansion of IoT devices. This landscape and history of breaches has given rise to immense and numerous consumer concerns with how, why, and what data is being used. Regulations exist for specific countries and intra-country regions, however, for the most part regulations are disjointed and less comprehensive for a number of areas. Overall, this has led to a large impasse between consumers and corporate and business interests. Consumers wish to have more knowledge and control over their data, and see privacy as a human right. Businesses see privacy as a privilege and commodity, and wish for this lack of regulation and innovation in the field of privacy and security to continue. The data seems to point to a recommendation that if overall social wellbeing is the goal, more regulations and cooperation should take place.

References

Baik, J. (2020) Data Privacy Against Innovation or Against Discrimination?: The Case of the California Consumer Privacy Act (CCPA) (September 1, 2020). Telematics and Informatics, 52. DOI:10.1016/j.tele.2020.101431 , Available at SSRN: https://ssrn.com/abstract=3624850

Kajabad, E. N. Ivanov, S. V., and Ramezanzade, N. (2020). "Customer Detection and Tracking By Deep Learning and Kalman Filter Algorithms," 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), 2020, pp. 1-6, doi: 10.1109/ICECCE49384.2020.9179224.

Hemker, S. Herrando, C. Constantinides, E. (2021) The Transformation of Data Marketing: How an Ethical Lens on Consumer Data Collection Shapes the Future of Marketing. Sustainability. 2021; 13(20):11208. https://doi.org/10.3390/su132011208

Luo, S., & Choi, T. M. (2022). E‐commerce supply chains with Considerations of Cyber‐Security: Should governments play a role? Production and Operations Management, 31(5), 2107–2126. https://doi.org/10.1111/poms.13666

Malan, J., Eager, J., Lale-Demoz, E., Ranghieri, G. C., & Brady, M. (2020). Framing the nature and scale of cyber security vulnerabilities within the current consumer internet of things (IoT) landscape. Centre for Strategy & Evaluation Services LLP, 1-102.

Ballco, P., de-Magistris T., Caputo V. (2019). Consumer preferences for nutritional claims: An exploration of attention and choice based on an eye-tracking choice experiment, Food Research International, Volume 116, 2019, Pages 37-48, ISSN 0963-9969, https://doi.org/10.1016/j.foodres.2018.12.031. (https://www.sciencedirect.com/science/article/pii/S0963996918309785)

Listoken, S. (2017)"Does Industry Self-Regulation of Consumer Data Privacy Work?," in IEEE Security & Privacy, vol. 15, no. 2, pp. 92-95, March-April 2017, doi: 10.1109/MSP.2017.45.