How have online marketing practices defined rights to data privacy in the digital age?

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

Rehan Javaid

Spring 2023

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

Advisor

S. Travis Elliott, Department of Engineering and Society

STS Research Paper

Introduction

The World Wide Web has expanded its influence an unprecedented amount since its early days in the 1990s. Through its growth, the Web has developed roles that have defined its use today—one such role being that of an online marketplace. As businesses made their transition to the digital world, their methods of marketing quickly followed suit. Digital advertising has since engulfed the browsing experience on the internet today. On any website we go, we are met with a diverse array of advertisements specifically catered to our interests and browsing habits at the time. However, this marketing shift that appears to have benefitted both consumers and businesses has not done so without controversial tactics at play. Many of the major marketing strategies on the internet have developed around web tracking: an action which allows for anonymous tracking of a user as they browse between sites. Marketing firms use technologies such as that of the cookie— a file that stores data about a user—to provide businesses with potential customers to advertise their products to (Team, 2019). An average user is not told that their patterns are being tracked as they browse or that their data is profited from without consent (Patel, 2021). By tracking our paper trails as we browse websites on the internet, cookies—more specifically third-party cookies—collect increments of data about us in order to form a profile used for targeted advertising (CookieYes, 2022).

Increasing awareness of digital marketing malpractice resulted in a movement to advocate for digital privacy rights. Through government legislation such as the California Consumer Privacy Act (CCPA*)* in 2018 and most recently statements by tech giants *Apple* and *Google* to remove the ability to use third-party cookies from their platform browsers (Bergen, 2021), steps have been taken to actively uphold a user's right to the privacy of their online data.

While the recognition of a user's digital privacy online is an important step towards creating a more ethical internet, it teases the question as to whether digital privacy rights would have been defined to the extent that they are today had it not been for the controversial practices of the digital marketing industry. To dive into these topics, this paper will cover the various techniques of data-usage and collection used in digital marketing for advertising today. Furthermore, it will analyze various consumer-privacy laws—namely the California Consumer Privacy Act, General Data Protection Regulation, EU Digital Services Act, and the Draft Online Safety Bill—that have been passed around the world to define privacy rights and protections online. This work will help to understand how online privacy came to be recognized today, and how legislation can assist in proactively protecting it from future data misuse.

STS Framework

In order to conduct this analysis, the STS framework that will be used is the social construction of technology (SCOT) theory developed by Trevor Pinch and Wiebe Bijker (1987). The SCOT theory discusses how human action shapes technology, and further that the success of a technology is dependent on the relevant social groups that interact with it. How a technology is adopted and used are key elements of the SCOT theory. One of the best examples of SCOT theory applied, comes from Pinch and Bijker in their 1987 book, *The Social Construction of Technological Systems.* Pinch and Bijker discuss SCOT in the context of the design of the bicycle: how it took people using the bicycle and social perceptions of the product to get it to where it is today (Bijker et al., 1987). Those who saw bicycles as unsafe influenced safety features to be added to the bicycle such as brakes and lights. Those who regularly used their bicycle for long distances wanted particular seat and grip designs. The technology has shaped itself to adapt to the desires of society upon its adoption into society.

In a similar case, the SCOT theory has applications for analyzing digital marketing technologies. SCOT will be implemented in this analysis in order to understand how human actors on the internet have shaped digital marketing technologies today in response to their increased demands for online privacy. This will be achieved by analyzing how certain technologies have changed after the implementation of digital privacy laws around the world.

Early Uses of the Web for Marketing

The earliest forms of marketing on the web date to the mid-90s. At the time, information sharing on the internet was limited and with the web still a fairly new technology, the data that could be used by businesses to get an understanding of their customers was restricted (Monnappa, 2023). Most businesses online presence at this time, if any, were simply websites to advertise themselves. Yet still, information on consumers could be obtained through certain means. Some businesses offered sign-up opportunities on their sites to offer customers rewards and special offers if they provided an email address. The information entered in these sign-up forms could be stored within a database and could provide businesses with a direct line of communication to their customers (Heinen, 1996). Online discussion groups have also been mentioned as a historically useful means for businesses to gain insight on customers—their experiences with products, and their preferences (Hoffman et al., 1995). Businesses offering the ability to make online purchases were able to gain the most useful information on their customers. These early businesses could harness of the power of stored sales data to obtain "a singular view of each customer" with information such as "client's likes and dislikes" (Xu et al., 2002). In 1995, DoubleClick Inc. was founded. This company provided space for advertisers to purchase banner ads (Jain, 2020).

The new millennium saw many new additions to the digital marketing landscape. On October 23, 2000, Google launched Google AdWords. This marked one of the first times ever that a browser was able to recommend user targeted advertisements by displaying advertisements based on keywords from a user's Google search (Vogal et al., 2000). A 2003 paper mentions the use of the web cookie, discussing how they can store "details concerning a transaction, as well as details concerning the visitor's activities at the Web site" (McDonald et al., 2003). This implies cookie-use in marketing starting to come into play. The arrival of Web 2.0 in early 2004 saw the rise of dynamic websites and social networking websites. With it came a way for businesses to interact more closely with their customers and magnitudinous increases in the amount of data present on the internet (Liu, 2009). It was during this time that the third-party cookie started to gain popularity amongst marketers.

Recognizing how society adopted and adjusted to a more interactive lifestyle on the internet, marketers recognized the new opportunities that this heightened interactivity presented in terms of available data. With the growth of social media and the expansion of the web provoking an onslaught of new users, "advertisers and marketers realized they could use cookies to track users across multiple websites and to gather data about their browsing behavior and interests" (Liu, 2009). User-specific targeted advertisements began to unfold, and the paper trail that every user of the web left behind became leveraged.

As marketers continued to make use of the ever-increasing consumer data present on the web, the rise of the smartphone created an entirely new landscape for which to adapt digital marketing practices. For one, smartphones have been the principal agents for creating a society in which "people are connected to the internet at any time and from anywhere" (Johnston, 2023). The unique quality of smartphones to not only receive but transmit information gave marketers

much more detailed information on their clientele (Johnston, 2023). Through means such as location sharing, companies are able to obtain data on the types of places their customers visit as an example (McFarlane, 2022).

Businesses became eager to adapt their marketing practices in order to be able to obtain this information. Recognizing the demand for this new, more-detailed data, social media giants such as Meta and Twitter became some of the main sources of supply. Lending data about their users to businesses for advertising became common practice and drastically shifted the operations of many social media sites (Thompson et al., 2019). As McFarlane mentions in his 2022 paper, the adoption of smartphones marked an era in which the user of the product became the product (McFarlane, 2022).

Digital Marketing Techniques Today

Today, cross-site tracking via the use of third-party cookies is one of the main ways advertisers are able to personalize ad recommendations online (Gozman, 2022). In a research study from Statista conducted on data from 2021, roughly 51% of marketing participants stated that "third-party cookies were very important for their current marketing strategy as they made up a majority of the data their company used" (Statista, 2022). In addition, methods of data collection like *deep packet inspection, history sniffing*, and *scraping* have also been mentioned as practices of data collection to assist the formation of the profile made about a user for targeting (Christiansen, 2011). Deep packet inspection allows for the monitoring of network traffic. For the purposes of marketing, it serves a role in targeted advertising through the means in which it allows businesses to track browsing data (Book, 2018). History sniffing serves a similar role—using code to "determine whether a consumer has previously visited a Web page" (Culhane et al., 2012). Lastly, web scraping allows for automated scanning of HTML code to retrieve a

desired piece of information asked for by a user (Ermakovich, 2022). Social media scraping is one of the most common use-cases of web scraping for digital marketing, allowing you to obtain information such as age, income, connections, and at what time a user is active (Ermakovich, 2022). The use of tracking pixels is another common method of data collection. Tracking pixels can be added to websites to obtain information such as a user's location and browsing history (Kelion, 2021). The distinction from cookies is the ability for cross-device targeting (Brenda, 2022). Such practices are commonly recommended to businesses as some the best ways to collect customer information. In a 2021 publication from the Harvard Business School *Business Insights* blog, *Online Tracking* with pixels and cookies and *Social Media Monitoring* are mentioned as 2 of 7 best ways to collect relevant customer data (Cote, 2021). A large marketing, sales, and customer service company, *Hubspot*, similarly recommends methods such as *Online Tracking* and paid ads on social media as the top ways to understand customers (Riserbato, 2021).

Responses to These Practices

Privacy concerns as a response to digital data-collection methods are on record as early as 2001. Miyazaki and Fernandez write about the privacy concerns associated with online retail and explain the legal and ethical concerns of "consumer information that is collected for commercial purposes" (Miyazaki et al, 2001). While some understood the risks the web brought for issues of data privacy, it is noted that "'privacy' was secondary to the focus on 'security'" (Andruss, 2022). Protecting passwords and stopping fraud was considered a more critical issue than what types of data businesses could obtain from users without consent.

The rise of Google, social media, and smartphones greatly changed the type of personally identifiable information that was available on the internet, yet many users were still unaware of

the ways their data was being used online and what types of information was being stored. This changed after an onslaught of major data breaches. Between 2012 and 2017 more than 130 data breaches brought public attention to the types of personal information obtainable online (Antamaniuk, 2021). In the infamous Yahoo data breach of 2013, roughly three billion accounts were compromised providing access to names, email addresses, and passwords (Sushko, 2021). Users became more aware of what kinds of information about them exist online.

This awareness translated over to the concern of how this information was being used without consent. Pew Research Center revealed that "86% of internet users have taken steps online to remove or mask their digital footprints" in a 2016 study. In 2017, Sarah West introduced the idea of *data capitalism*, bringing to the public eye the imbalance that exists between the user and their lack of knowledge of what information about them is collected and the "actors who have access and the capability to make sense of information" (West, 2017). Heightened awareness of the threats to digital privacy taking place on the web sparked calls for change and legal protection from further malpractice in data collection. The following sections look into the General Data Protection Regulation of 2018, the California Consumer Privacy Act of 2018, the 2020 EU Digital Services Act, and lastly the 2021 draft Online Safety Bill.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation is a 2018 legislation that ensures data protection to the UK and Europe. The legislation presents rules for how personal data is to be collected and processed by companies and which situations warrant the collection of personal data. Most importantly, it defines a specific set of privacy rights for users.

Article 4 of the GDPR provides a definition of personal data. The GDPR states that personal data is “any information relating to an identified or identifiable natural person” (Wolford, 2022). Additionally, this definition is defined further to include any information that could be used to indirectly identify—ID numbers, biometrics, etc.

Article 5 lists specific ways to handle and process data. Some of the most important of these include a principle that personal data shall be “processed lawfully, fairly and in a transparent manner” and further be “collected for specific, explicit and legitimate purposes” (Wolford, 2022). Of additional importance is that personal data must be “adequate, relevant and limited to what is necessary (Wolford, 2022).

` On the issue of consent, the GDPR defines rules about what counts as consent. It states that “consent must be ‘freely given, specific, informed and unambiguous” and mentions that “data subjects can withdraw previously given consent whenever they want, and you have to honor their decision” (Wolford, 2022).

Lastly, regarding individual privacy rights, the GDPR specifically lists the rights of a “data subject”. These are the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, and the right to data portability, the right to object, and rights in relation to automated decision making and profiling.

California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act is a legislation passed in 2018 that lists requirements for “identifying, managing, securing, tracking, producing, and deleting consumer privacy information” (Diamond, 2019). The act provides protections to all residents of California and states that its requirements must be strictly followed by all “for-profit businesses that collect

and control California residents' personal information" and "do business in the State of California" (Diamond, 2019).

In regards to privacy rights specified by the CCPA, there are five. These are 1) To know what personal information is collected about them 2) To know whether and to whom their personal information is sold/disclosed, and to opt-out of its sale 3) To access their personal information that has been collected 4) To have a business delete their personal information 5) To not be discriminated against for exercising their rights under the act (Diamond, 2019).

EU Digital Services Act (DSA)

The EU Digital Services Act is a legislation initially presented in 2020 and currently getting formal approval to come into law in 2024. One of its goals is to increase the transparency of big tech to their consumers. In the realm of digital marketing, this means that businesses must provide information on ad targeting regarding the sponsor and the advertiser and why it has targeted a user. Additionally, the act would completely ban certain targeted advertisements such as those that target minors (Browne, 2022).

In addition, the act provides a set of obligations that large businesses and search engines must abide by. These include activities such as publishing their terms and conditions in the official languages of all Member States serviced and conducting annual assessments of "systemic risks" present within their platforms regarding misinformation (Browne, 2022). Failure to abide by any conditions listed result in fines.

Online Safety Bill

The UK Online Safety Bill is currently in debates to become law by the British Houses. Many of the goals of this legislation are similar to those of the Digital Services Act, to increase

transparency and reduce fraudulent content (Lomas, 2022). In the scope of digital marketing, the bill recently adopted a revision that makes social media sites responsible for the prevention of targeting with fraudulent advertisements, which if effective could help reduce the amount of user data being sent to businesses with malicious intent (Lomas, 2022).

Discussion

The legislation currently at play is an important mark of the demand for the protection of user data on the internet. The role that digital marketing played in leading to the development of these rights is evident from the efforts of these laws to directly combat issues of transparency in data collection. These technologies have driven marketing on the web since its early years, with marketing tactics such as the use of cookies and pixels directly responsible for nonconsensual data collection for the benefit of business intelligence.

Much of this legislation has proven effective as well. With the GDPR in effect, websites and services with customers in the EU have had to make conscious efforts to comply with its principles. For example, businesses now have separate marketing consent distinct from a Terms and Conditions agreement to decide whether or not consumers want to receive updates and advertisements from them (Olsen, 2022). Additionally, the ability to opt-out of a previously opted-in agreement has become increasingly commonplace. Privacy agreements are also openly presented on websites collecting any form of consumer data. These changes show how the cynical view of covert marketing operations online has begun to spark change in the industry. As SCOT theory states, user perception and interaction with marketing technology has begun to shape the technology.

Since legislation proves an effective means of forcing user privacy to be recognized on the internet today, it begs the question as to why it is the case that the legislation that exists today developed as a reactionary means to the actions of the marketing industry rather than as a preemptive defense against them. Perhaps the strongest argument to be made is that there was no possible way to predict the extent to which technology would progress in as small a timeframe as 10-20 years. One could argue that establishing data protection rights in the early days of the web may have been ineffective since there would have been no way to gauge how many different sources of data would exist today. How social media blew up and became such a key source of consumer data almost overnight is an example of such unpredictability.

Seeing how marketing technology has evolved since the passage of legislation through the lens of the SCOT theory, however, provides support for the preemptive development of widespread digital privacy rights today. The SCOT theory states that the success of a technology is dependent on the relevant social groups that interact with it. Before—without recognition and respect of a user's right to online privacy—the marketer was the main source of interaction with marketing technology. Society failing to see marketing tactics as potentially problematic meant the marketer was free to do with their technology as they saw fit. Web users had little knowledge of how their data was being used and to what extent. The user merely had to use the web for the technologies driving marketing data-collection practices to work effectively.

However, since the recognition of digital privacy rights through legislation and widespread advocacy over time, the level of direct interaction between the user and marketing technologies has increased. For example, by defining users' right to consent, users now directly interact with marketing technology by seeing what data it is collecting from them and deciding to allow/disallow the technology to function accordingly. The stake of the user in digital marketing

has changed, and as a result marketing technologies have had to adapt to recognize this increased stake and demand for privacy. As society began to demand online privacy, technologies grew to become more transparent. Just as the principles of the SCOT theory describe, digital marketing technology today is a textbook example of how the user can define a technology through their interaction with and perception of it.

Defining widespread, federal laws recognizing digital privacy today means that marketers will continue to have to comply with the societal recognition of privacy online or else limit the effectiveness of the current technologies used for data-collection. By defining widespread privacy rights today, it is possible to shape the technologies created for the collection of consumer data moving forward.

Conclusion

To conclude, the analysis conducted of the research question revealed that digital marketing practices fostered the birth of digital privacy rights through the use of personal data without permission, and furthermore that current legislation to handle this misuse has proven to be effective in recognizing user privacy online. Currently there are no federal privacy laws in the United States regarding data collection online. Failing to establish clear, widespread privacy rights as technology becomes more intelligent and data collection tactics become less transparent will prove to limit the ownership that internet users have over their own data. Taking a proactive measure to define federal rights to privacy and how personal data can be used online will shape the technologies that follow to recognize these rights and create a more ethical internet.

References

Andruss, R. (2022). *A brief history of data privacy, and what lies ahead*. Skyflow. Retrieved March 17, 2023, from https://www.skyflow.com/post/a-brief-history-of-data-privacy-and-what-lies-ahead

Atamaniuk, M. (n.d.). *20 years in digital privacy: How the definition has evolved*. Clario. Retrieved March 17, 2023, from https://clario.co/blog/privacy-definition-over-years/

Bijker, W. E., Hughes, T. P., & Pinch, T. (1987). The social construction of technological systems: New Directions in the sociology and history of technology. MIT Press.

Book, C. (2018). *What is deep packet inspection? how it works, use cases for DPI, and more*. Digital Guardian. Retrieved March 17, 2023, from https://www.digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more

Breda, J. van. (2022, July 18). *Pixels and cookies – remarketing explained*. The Negotiator. Retrieved March 17, 2023, from https://thenegotiator.co.uk/pixels-and-cookies/

Browne, R. (2022, April 23). *Eu agrees on landmark law aimed at forcing Big Tech firms to tackle illegal content*. CNBC. Retrieved March 17, 2023, from https://www.cnbc.com/2022/04/22/digital-services-act-eu-agrees-new-rules-for-tackling-illegal-content.html

Christiansen, L. (2011). Personal privacy and internet marketing: An impossible conflict or a marriage made in heaven? *Business Horizons*, *54*(6), 509–514. https://doi.org/10.1016/j.bushor.2011.06.002

Cote, C. (2021, December 2). *7 data collection methods in Business Analytics*. Business Insights Blog. Retrieved March 17, 2023, from https://online.hbs.edu/blog/post/data-collection-methods

Culhane, J., Furletti, M., & Kaplinsky, A. (2012, December 13). *FTC settles 'history sniffing' charges against online advertising network*. JD Supra. Retrieved March 17, 2023, from https://www.jdsupra.com/legalnews/ftc-settles-history-sniffing-charges-a-97336/

Diamond, M. (n.d.). *Quick overview: Understanding the california consumer privacy act (CCPA)*. Quick Overview: Understanding the California Consumer Privacy Act (CCPA) | Association of Corporate Counsel (ACC). Retrieved March 17, 2023, from https://www.acc.com/resource-library/quick-overview-understanding-california-consumer-privacy-act-ccpa#

Ermakovich, S. (2022, April 8). *How to use web scraping for marketing and product analytics*. VentureBeat. Retrieved March 17, 2023, from https://venturebeat.com/datadecisionmakers/how-to-use-web-scraping-for-marketing-and-product-analytics/

Heinen, J. (1996). Internet marketing practices. *Information Management & Computer Security*, *4*(5), 7–14. https://doi.org/10.1108/09685229610153120

Hoffman, D. L., Novak, T. P., & Chatterjee, P. (1995). Commercial scenarios for the web: Opportunities and challenges. *Journal of Computer-Mediated Communication*, *1*(3). https://doi.org/10.1111/j.1083-6101.1995.tb00165.x

Jain, A. (2020, December 14). *DoubleClick: An acquisition that skyrocketed Google's ad business*. The Strategy Story. Retrieved March 17, 2023, from https://thestrategystory.com/2020/12/14/google-doubleclick-acquisition/

Johnston, M. (2023, January 28). *How smartphones changed advertising*. Investopedia. Retrieved March 17, 2023, from https://www.investopedia.com/articles/personal-finance/062315/how-smartphones-are-changing-advertising-marketing.asp

Kelion, L. (2021, February 17). *'spy pixels in emails have become endemic'*. BBC News. Retrieved March 17, 2023, from https://www.bbc.com/news/technology-56071437

Liu, Y., & Ji, S. (2009). Gathering Customer ’s Demand Data through Web 2.0 Community: Process and Architecture. *AIS Electronic Library*.

Lomas, N. (2022, March 9). *UK expands online safety bill to cover scam ads and eyes wider reforms*. TechCrunch. Retrieved March 17, 2023, from https://techcrunch.com/2022/03/09/online-safety-bill-scam-ads/

McDonald, H., & Adam, S. (2003). A comparison of online and postal data collection methods in Marketing Research. *Marketing Intelligence & Planning*, *21*(2), 85–95. https://doi.org/10.1108/02634500310465399

McFarlane, G. (2022, December 19). *How facebook (meta), Twitter, social media make money from you*. Investopedia. Retrieved March 17, 2023, from https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx

MIYAZAKI, A. N. T. H. O. N. Y. D., & FERNANDEZ, A. N. A. (2001). Consumer perceptions of privacy and security risks for online shopping. *Journal of Consumer Affairs*, *35*(1), 27–44. https://doi.org/10.1111/j.1745-6606.2001.tb00101.x

Monnappa, A. (2023, February 8). *The history and evolution of Digital Marketing*. Simplilearn.com. Retrieved March 17, 2023, from https://www.simplilearn.com/history-

and-evolution-of-digital-marketing-article#:~:text=the%20most%20ground.-,History%20of%20Digital%20Marketing,this%20information%20over%20the%20web

Olsen, N. (2022, July 1). *The GDPR's impact on digital marketing*. Privacy Policies. Retrieved March 17, 2023, from https://www.privacypolicies.com/blog/gdpr-digital-marketing/#How_The_Gdpr_Is_Changing_Targeted_Ads

Riserbato, R. (2021, June 9). *The plain English guide to customer data collection*. HubSpot Blog. Retrieved March 17, 2023, from https://blog.hubspot.com/service/customer-data-collection

Sushko, O. (n.d.). *10 data breaches of the Decade: How famous brands let us down*. Clario. Retrieved March 17, 2023, from https://clario.co/blog/top-data-breaches-of-2010s/

Thompson, S. A., & Warzel, C. (2019, December 20). *Smartphones are spies. here's whom they report to.* The New York Times. Retrieved March 17, 2023, from https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html

Vogal, K., & McCaffrey, C. (2000, October 23). Google Launches Self-Service Advertising Program [web log]. Retrieved 2023, from http://googlepress.blogspot.com/2000/10/google-launches-self-service.html.

Wolford, B. (2022, May 26). *What is GDPR, the EU's new Data Protection Law?* GDPR.eu. Retrieved March 17, 2023, from https://gdpr.eu/what-is-gdpr/

Xu, Y., Yen, D. C., Lin, B., & Chou, D. C. (2002). Adopting customer relationship management technology. *Industrial Management & Data Systems*, *102*(8), 442–452. https://doi.org/10.1108/02635570210445871