iS
CHANNEL

Data Privacy in the Age of Surveillance Capitalism

Cathal Greaney

MSc in Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

ABSTRACT

Ubiquitous information technologies such as smartphones enable the collection of users every digital action and allow private enterprises to commoditize a user's data. This leads to asymmetries of power between the users who share their digital actions and the corporations who can aggregate and analyse their data for profit. The benefits enjoyed by the users act as a justification for the loss of privacy resulting from this activity. In this article, I review the origins and core concepts of the surveillance capital business model and its effect on privacy and I discuss the potential dangers of an environment where a user's every digital action is recorded.

"We're at the beginning [of surveillance capitalism] not the end. We name it, we tame it. That's the work now. To reignite our democracy, wake it up, for this work of the 21st century" (Shoshana Zuboff, 2019)

"Dataism is a new ethical system that says, yes, humans were special and important because up until now they were the most sophisticated data processing system in the universe, but this is no longer the case" (Harari, 2016)

"Enterprise mobility affords great flexibility within the appropriate context, but also significant opportunities for extensive surveillance. Modern workers have anywhere to go, and nowhere to hide" (Sørensen, 2011)

Introduction

Almost everything we do online produces a digital record. When we make a call, send a message, buy a pizza or go for a jog our data is recorded and captured. Surveillance capitalism captures this personal behavioural data, translates it into predictions and sells those predictions into new markets that trade exclusively in behavioural futures (Zuboff, 2015). Is this scary and Orwellian and a precursor to internalized social controls, or merely continuing progress in the relentless drive towards a new age of "dataism" (Harari, 2016). Regardless of the political or technological viewpoint, surveillance capitalism is already enmeshed in our daily lives by means of smartphones, watches, fitness trackers and other ubiquitous information technologies. Our digital data has become a critical raw material and is analysed and sold to advertisers and used to enhance digital services, increase our digital participation and used to augment the existing government surveillance apparatus.

Enterprises, through similar mechanisms, can monitor workers every action (Sørensen, 2011). Firms even host 'microchip parties' (Agence France-Presse, 2018; Mills and Press, 2017), to convince employees to implant a tracker under their skin. Amazon carefully monitors their warehouse workers and if inefficiencies are detected they can be automatically cautioned (Bort, 2019). UPS drivers face similar scrutiny on their delivery routes (Goldstein, 2014). Within the political realm, Bloomberg reported that Facebook adapted its surveillance capitalism mechanisms to directly influence voters in the 2017 German national elections, controversially resulting in the AfD party getting a surprising increase in votes (Silver, 2017). In Brazil, political commentators argue that the winning candidate in the last presidential elections owed his victory in part to sophisticated use of social media (Leahy, 2018; Leahy and Schipani, 2018). However, it is worth noting that in the latter two cases mentioned, there was no indication that Facebook's motivations were political. As discussed later in this article, it was merely a side effect of their relentless pursuit of ever-increasing user engagement.

The techniques of surveillance capitalism are largely subliminal and shockingly effective in the manipulation of social behaviour (Zuboff, 2019). Surveillance capitalism's primary focus may be within the commercial sphere, but like traditional advertising, it can and is being applied to other spheres of influence. In order to understand surveillance capitalism, it is helpful to first consider its origins.

The origins of surveillance capitalism

Surveillance capitalism traces its roots to Google's reaction to the 1999-2000 dot-com bust. Up to that point, there was a reasonably balanced power relationship between the nascent web companies who needed users and the users themselves who benefitted from the emerging online services. The phrase 'if you're not paying for the product, you are the product' (Serra and Weyergraf-Serra, 1980) was sometimes co-opted to describe this business model. When the dot-com bubble burst in April 1999 investors threatened to withdraw support unless a profitable business model was applied. In response, Google adopted a straightforward 'keyword search'

Corresponding Author
Email Address: cathal@irishapps.com

based advertising business model (Brin and Page, 1998). Advertisers would choose keywords and when users conducted a Google search using these same keywords they would see the adverts. In parallel to this, there was a realization that Google's user-generated collateral search data had tremendous predictive value. Google applied their considerable compute ability and proprietary access to this data to predict the kinds of ads their users were likely to click on. It became known as the "click through rate" (Lohtia et al., 2003) and represented the perceived relevance of an ad. Google offered this new predictive service to advertisers in a black box fashion and advertisers accepted it. The phrase 'you are the product' can be changed to 'your data surplus and predictive behaviours are the product'. In March 2008, Facebook hired Sheryl Sandberg to spearhead their adoption of the surveillance capital business model pioneered by Google. This represented an inflection point and saw the accelerated adoption of surveillance capital techniques by major players such as Microsoft, Netflix, Uber, and many others.

During this transitionary period, internet companies switched from selling products online, to the harvesting of their user's data as the primary source of revenue. The mechanisms of this new business model were largely kept invisible to users. The benefits of a globally connected community operating in a transparent manner were highlighted while the risks of power asymmetry, social control, and exploitation of users' data remained obscured.

This period of the dot-com bust and emergence of surveillance capitalism is well documented but poorly understood and barely theorised. The remainder of this article will examine information systems concepts related to data privacy and surveillance capitalism and discuss the power dynamics shaping this evolving paradigm.

A Definition of digital privacy

Digital or information privacy is a difficult concept to define. It relates to the accessibility of personal information. Services such as Gmail, Facebook, Instagram and WhatsApp harvest our personal data for commercial gain and users seem happy to participate. The development of services that rely on surveillance and users' responses to these services has challenged the traditional definition of privacy. Information systems scholars have offered some guidance. Bélanger and Crossler (2011) define privacy as "the desire of individuals to control or have some influence over data about themselves". Smith et al. (2011) explore definitions of privacy as a right or as a commodity. They argue that the traditional view of general privacy as a human right is ill-suited to the commercial world and that within this context a privacy paradox is observed between a user's expressed wishes for privacy and their contradictory consumer behaviours.

This privacy paradox phenomenon refers to a user's express wish for digital privacy while willingly revealing personal information online (Dinev, 2014; Smith et al., 2011). Following this observation, it is useful to think of privacy as a commodity (Fuchs, 2012) in which it is not considered an absolute value, but can be assigned an economic value. Privacy benefit is a related concept and refers to the rewards gleaned from providing personal information to firms, including financial gain and personalization of services (Smith et al., 1996; Caudill and Murphy 2000; Hann et al. 2008; Phelps et al. 2000; Xu et al. 2010). If an individual thinks their interactions with a firm will result in the unwanted release of their personal information it is referred to as privacy risk (Featherman and Pavlou 2003; Malhotra et al. 2004). Based on the success of Facebook and Google, it is reasonable to conclude that users perceived privacy benefit far outweighs their concerns over privacy risk. But to what extent are general users aware of the erosion of their privacy? In order to answer that question, we should consider the specific modes of collection being employed.

Commercial data collection companies are becoming increasingly invasive. Cookies and similar tracking artefacts are routinely placed on user's devices and facilitate the collection of large amounts of behavioural data. Keyboard and mouse input are recorded along with the recording of conversations through laptop and smartphone microphones and images are captured using devices cameras (Sipior et al., 2011). In the early 2000s when these practices were emerging there was little effort employed to inform the user of the level of tracking taking place. Over time the major smartphone platforms introduced notifications and explicit opt ins so that users had to agree before services or apps could record data using smartphones location capabilities, microphone or cameras. Based on this, it is reasonable to conclude that users are informed as to the extent their digital activates are being recorded. Zuboff (2019) argues that despite these opt in practices users privacy is being forcibly eroded. She recalls the philosopher Roberto Unger's warning of "the dictatorship of no alternatives" and argues that users have no choice but to cede their privacy in order to avoid practical digital exclusion regardless of the level of digital risk or privacy benefit. She goes on to discuss existing digital concepts such as 'digital ubiquity' through the lens of surveillance capitalism and introduces the concepts of 'digital instrumentarianism', 'instrumentarian power' and 'radical indifference'.

The Four Horsemen of Surveillance Capitalism

Digital instrumentarianism, digital ubiquity, radical indifference, instrumentarian power.

Digital instrumentarianism describes firms influencing our behaviour so that the predictability of our actions increases. Surveillance capital does not care about what we do, who we are or what our problems might be, so long as data can be captured and predictions can be extracted from it. Zuboff (2019) calls this "radical indifference", referring to the indifference of surveillance capitalism to an individual's actions, so long as predictive data can be gathered. Facebook's Andy Bosworth described it as:

*"…connecting people so deeply that anything that allows us to connect more people more often is *de facto* good… [not] for ourselves or for our stock price. It is literally just*

what we do. We connect people" (Andrew Bosworth, 2016)

Digital ubiquity is the core enabler for surveillance capitalism. Zuboff describes it as an intense, thick surround of digital instrumentarianism which subliminally shapes a user's behaviour in a direction that favours a firm's commercial outcomes. Surveillance capitalism will encourage actions that make a user more predictable. The familiar example of the 'filter bubble' (Nguyen et al., 2014) in the hands of surveillance capitalists does not just increase user engagement through enhanced user experience. Its main objective is to increase a user's predictability in the online world through altered behaviour. The same devices that allow us to monitor, can now be used to actuate, both in the online world and increasingly in the physical world. Data scientists call this monitoring and actuation.

One of the best early examples of monitoring and actuation was provided by Kramer et al. (2014) who conducted a massive scale experiment in collaboration with the Facebook news feed team. They introduced an "emotional contagion" (Hatfield et al., 1993) by reducing the volume of positive expressions within a user's news feed. As a result, they observed the person producing fewer positive posts. To illustrate a real world context, Zuboff (2019) cites the Pokémon Go app. Pokémon Go is a mobile game that uses augmented reality to project Pokémon cartoon characters within physical locations. In order to progress through the game, the user must find these virtual characters by going to physical locations. It uses the same processes as online targeted advertising, but in this case business customers pay for future behaviour in the real world. Users are directed towards specific restaurants or shops outside of their conscious awareness. Pokémon Go is a good example of monitoring and actuation and how surveillance capitalists have moved away from the laptop and now rely on the mobile phone as the chief supply chain interface for its raw materials. In the next section, I discuss the role of the smartphone as the primary tool for data capture.

Smartphones and privacy

Surveillance capital leads to intense competition for behavioural surplus and prediction products and it is no longer enough to have a high volume of surplus (scale). A variety of surplus (scope) is also needed. The user's mobile phone becomes the critical tool with economies of scope working in two dimensions (Anderson, 2019; Zuboff, 2019). Firstly, to extend out as far as possible by capturing locations and actions and then extending as deeply as possible by capturing feelings and emotions through the analysis of user images, videos and voice (Cambria, 2016). But the most predictive surplus comes from intervening in users activities, and herding users in specific directions (Wykes, 2019). This competition has resulted in pressures being applied to new and established businesses to leverage their data to create products for digital prediction markets (Shimp, 2017). In the age of surveillance capitalism, the primary goal is to maximize user engagement while minimizing the awareness of dataveillance activities happening in parallel. The term "dark patterns" is used in the app design community to describe design patterns that are not in the user's best interests or not optimized for the user (Zagal et al., 2013). In the case of surveillance capitalism, an app's user interface is optimized for data capture rather than for optimal user experience. Faced with the competitive pressures of surveillance capitalism, app designers may have to prioritize data capture over user experience in order to remain competitive in the market place.

Some scholars have proposed steps to safeguard digital privacy. Cavoukian's (2012) Privacy by Design (PbP) framework can be used when considering digital privacy and includes principles such as privacy by default, privacy embedded in core architecture, secure communications and transparency and respect for user privacy. PbD principles encourage the use of methods such as encryption during transmission which would significantly enhance security, even when using platforms controlled by surveillance capitalist firms. The metadata would still be exposed to data harvesting, but the user data would enjoy significant protection. Data prediction markets provide motivation for malware and phishing attacks (Felt et al., 2011). Malware and phishing attacks are used to harvest data for sale on the data markets (Bhandari et al., 2017; Jain and Shanbhag, 2012; Wright et al., 2014) and in these cases, following PbD guidelines by increasing the security robustness of apps and awareness of attack vectors could enhance users privacy.

Instrumentarian power

To complete our discussion of surveillance capitalism it is worth considering the power dynamics in play. Social and political study of technology is core to Information Systems research (Eaton et al., 2015; Markus, 1983; Orlikowski, 1991; Sørensen, 2011). Surveillance capitalism works through the medium of all of the digital instrumentation while turning the user into instruments of others gain. For this dual reason, Zuboff (2019) uses the term "instrumentarian power" to describe surveillance capitalism's instrumental relationship with its user base. Instrumentation is used at arm's length to shape behaviour. The user is not aware or afraid of it. Zuboff (2019) considers surveillance capitalism to be anti-democratic and makes a convincing case for her views. She considers the potential benefits that may accrue as secondary to how they would be achieved and that getting a great outcome in an anti-democratic fashion is not good for our society. Extreme asymmetries of knowledge result in extreme inequalities of power (Zuboff, 2019). Computation replaces politics. Resistance is not possible because we're not aware of what's happening. Computational certainty may not be compatible within the democratic social context.

Other social scientists have taken a different view. Harari (2018, 2016) calls surveillance capitalism a subset of 'dataism' and describes it as an emerging ideology in which "information flow [is the] supreme value". He goes on to describe the historical advantages

of democracy in terms of data flow and distributed communication and power sharing. He reasons that democracy flourished in the 20th century because it adopted a more decentralized communications and power system than competing totalitarian systems and points out that democracy or more specifically, liberal democracy has gone through several cycles of crises and regeneration and has the potential to adapt to new forms of emerging power based on data.

When examining power dynamics there are obvious parallels between the traditional advertising industry and surveillance capitalism. When advertising emerged after the First World War, it shared the same characteristics as surveillance capitalism does now. It was an emerging phenomenon based on cutting edge technology and used by private firms as a means of passive manipulation and control and became known as "manufactured consent" (Herman and Chomsky, 2010). Rather than subverting democracy, it instead became a vital tool for democracy in the 20th century.

Conclusion

Harari reminds us that history is not deterministic. "The same technological breakthroughs can create very different kinds of societies". Zuboff has highlighted an important phenomenon and provides a wakeup call to the academic, professional and political establishments. The field of Information Systems is well placed to illuminate the emerging field of commercial data surveillance as it transforms our society and influences our everyday actions. Smith et al. (2011) warn that the practice of commercial sharing of data by Facebook, Google and other major tech firms risks eventually alienating users. With increased awareness of the pervasiveness of surveillance capitalism, public opinion may shift and demand may emerge for products that better protect user's privacy. For example, users may choose to pay for an encrypted email service such as ProtonMail rather than using Gmail. Noted venture capitalist Roger McNamee (2019) was instrumental in introducing surveillance capitalism into Facebook and is now vocal in his opposition to these practices and believes they will ultimately be self-destructive to the firm due to user backlash. Some scholars have illuminated other negative effects such as algorithmic discrimination, hidden political influence and the expansion of state influence on everyday lives (Crawford and Schultz, 2014; Noble, 2018).

This article has focused on the more opaque aspects of surveillance capitalism, some of which could be interpreted as negative social developments. There are overwhelmingly positive aspects of recent technological progress in areas associated with data collection and open communication. Ubiquitous networking provides unprecedented access to educational opportunities and other knowledge based services and digital experiences that enhance everyday lives. New forms of consumer power have emerged that disrupt parasitic industry practices and deliver enhanced value to consumers. As discussed earlier, there are asymmetries of power at play. Facebook, Microsoft, Google and Amazon are at the forefront but there is little evidence they or other major players have abused this power imbalance beyond their corporate profit motives. These imbalances can be combatted through the use of accessible encryption and anonymization services. Should abuses occur on a significant scale then it is reasonable to assume that users would respond by employing some of these anti-surveillance techniques or by simply boycotting the offending services in favour of more secure modes of communication.

However, the concerns expressed in this article about the secretive aspects of surveillance capitalism should not be dismissed as an overreaction or paranoia. Despite the rhetoric of transparent communications that the major players extol, they operate in a zealously guarded and secretive manner. The vast data centre infrastructure needed is only available to a select few. Algorithms used to collect data and influence users are purposefully hidden from view and treated as prized internal IP. The technology of surveillance capital is only available to the biggest handful of players.

References

Agence France-Presse, 2018. Why thousands of people in this country got microchip implants - party [WWW Document]. South China Morning Post. URL https://www.scmp.com/news/world/europe/article/2145896/thousands-people-sweden-get-microchip-implants-new-way-life (accessed 4.28.19).

Anderson, T., 2019. Challenges and Opportunities for use of Social Media in Higher Education. J. Learn. Dev. - JL4D 6.

Bélanger, F., Crossler, R.E., 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Q. 35, 1017–1041. https://doi.org/10.2307/41409971

Bhandari, S., Jaballah, W.B., Jain, V., Laxmi, V., Zemmari, A., Gaur, M.S., Mosbah, M., Conti, M., 2017. Android inter-app communication threats and detection techniques. Comput. Secur. 70, 392–421. https://doi.org/10.1016/j.cose.2017.07.002

Bort, J., 2019. Amazon's warehouse-worker tracking system can automatically pick people to fire without a human supervisor's involvement [WWW Document]. Bus. Insid. URL https://www.businessinsider.com/amazon-system-automatically-fires-warehouse-workers-time-off-task-2019-4 (accessed 4.28.19).

Brin, S., Page, L., 1998. The anatomy of a large-scale hypertextual Web search engine. Comput. Netw. ISDN Syst., Proceedings of the Seventh International World Wide Web Conference 30, 107–117. https://doi.org/10.1016/S0169-7552(98)00110-X

Cambria, E., 2016. Affective Computing and Sentiment Analysis. IEEE Intell. Syst. 31, 102–107. https://doi.org/10.1109/MIS.2016.31

Cavoukian, A., 2012. Privacy by Design [Leading Edge]. IEEE Technol. Soc. Mag. 31, 18–19. https://doi.org/10.1109/MTS.2012.2225459

Crawford, K., Schultz, J., 2014. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. Boston Coll. Law Rev. 93–128.

Dinev, T., 2014. Why would we care about privacy? Eur. J. Inf. Syst. 23, 97–102. https://doi.org/10.1057/ejis.2014.1

Eaton, B., Elaluf-Calderwood, S., Sorensen, C., Yoo, Y., 2015. Distributed tuning of boundary resources: the case of Apple's iOS service system. MIS Q. Manag. Inf. Syst. 39, 217–243.

Felt, A.P., Finifter, M., Chin, E., Hanna, S., Wagner, D., 2011. A Survey of Mobile Malware in the Wild, in: Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, SPSM '11. ACM, New York, NY, USA, pp. 3–14. https://doi.org/10.1145/2046614.2046618

Fuchs, C., 2012. The Political Economy of Privacy on Facebook. Telev. New Media 13, 139–159. https://doi.org/10.1177/1527476411415699

Goldstein, J., 2014. To Increase Productivity, UPS Monitors Drivers' Every Move [WWW Document]. NPR.org. URL https://www.npr.org/sections/money/2014/04/17/303770907/to-increase-productivity-ups-monitors-drivers-every-move (accessed 4.28.19).

Harari, Y.N., 2018. 21 Lessons for the 21st Century. Random House Publishing Group.

Harari, Y.N., 2016. Homo Deus: A Brief History of Tomorrow. Harvill Secker.

Hatfield, E., Cacioppo, J.T., Rapson, R.L., 1993. Emotional Contagion. Curr. Dir. Psychol. Sci. 2, 96–100. https://doi.org/10.1111/1467-8721.ep10770953

Herman, E.S., Chomsky, N., 2010. Manufacturing Consent: The Political Economy of the Mass Media. Random House.

Jain, A.K., Shanbhag, D., 2012. Addressing Security and Privacy Risks in Mobile Applications. IT Prof. 14, 28–33. https://doi.org/10.1109/MITP.2012.72

Kramer, A.D.I., Guillory, J.E., Hancock, J.T., 2014. Experimental evidence of massive-scale emotional contagion through social networks. Proc. Natl. Acad. Sci. 111, 8788–8790. https://doi.org/10.1073/pnas.1320040111

Leahy, J., 2018. FT Surging support for Brazil's Lula da Silva unnerves markets [WWW Document]. Financ. Times. URL https://www.ft.com/content/e20c2888-a67f-11e8-8ecf-a7ae1beff35b (accessed 4.28.19).

Leahy, J., Schipani, A., 2018. FT How social media exposed the fractures in Brazilian democracy [WWW Document]. Financ. Times. URL https://www.ft.com/content/8c08654a-c0b1-11e8-8d55-54197280d3f7 (accessed 4.28.19).

Lohtia, R., Donthu, N., Hershberger, E.K., 2003. The Impact of Content and Design Elements on Banner Advertising Click-through Rates. J. Advert. Res. 43, 410–418. https://doi.org/10.1017/S0021849903030459

Markus, M.L., 1983. Power, Politics, and MIS Implementation. Commun ACM 26, 430–444. https://doi.org/10.1145/358141.358148

McNamee, R., 2019. Zucked: Waking Up to the Facebook Catastrophe. Penguin Publishing Group.

Mills, E., Press, A., 2017. Tech company holds "chip party" to implant microchips in more than 40 workers. The Telegraph.

Nguyen, T.T., Hui, P.-M., Harper, F.M., Terveen, L., Konstan, J.A., 2014. Exploring the Filter Bubble: The Effect of Using Recommender Systems on Content Diversity, in: Proceedings of the 23rd International Conference on World Wide Web, WWW '14. ACM, New York, NY, USA, pp. 677–686. https://doi.org/10.1145/2566486.2568012

Noble, S.U., 2018. Algorithms of Oppression: How Search Engines Reinforce Racism. NYU Press.

Orlikowski, W.J., 1991. Integrated information environment or matrix of control? The contradictory implications of information technology. Account. Manag. Inf. Technol. 1, 9–42. https://doi.org/10.1016/0959-8022(91)90011-3

Serra, R., Weyergraf-Serra, C., 1980. Richard Serra, Interviews, Etc., 1970-1980. Hudson River Museum.

Shimp, G., 2017. How Digital Transformation Is Rewriting Business Models [WWW Document]. URL https://www.digitalistmag.com/digital-economy/2017/04/19/digital-transformation-rewriting-business-models-05042457 (accessed 4.29.19).

Shoshana Zuboff, 2019. Democracy Now Interview with Shoshana Zuboff.

Silver, V., 2017. The German Far Right Finds Friends Through Facebook.

Sipior, JaniceC., Ward, BurkeT., Mendoza, RubenA., 2011. Online Privacy Concerns Associated with Cookies, Flash Cookies, and Web Beacons. J. Internet Commer. 10, 1–16. https://doi.org/10.1080/15332861.2011.558454

Smith, H.J., Dinev, T., Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review. MIS Q. 35, 980-A27.

Sørensen, C., 2011. Enterprise Mobility: Tiny Technology with Global Impact on Work [WWW Document]. URL https://www.dawsonera.com/readonline/9780230306202 (accessed 1.15.19).

Wright, R.T., Jensen, M.L., Thatcher, J.B., Dinger, M., Marett, K., 2014. Research Note—Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. Inf. Syst. Res. 25, 385–400. https://doi.org/10.1287/isre.2014.0522

Wykes, T., 2019. Racing towards a digital paradise or a digital hell? J Ment Health 28, 1–3. https://doi.org/10.1080/09638237.2019.1581360

Zagal, J.P., Björk, S., Lewis, C., 2013. Dark Patterns in the Design of Games. Presented at the Foundations of Digital Games 2013.

Zuboff, S., 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Profile Books.

Zuboff, S., 2015. Big other: Surveillance Capitalism and the Prospects of an Information Civilization. J. Inf. Technol. 30, 75–89. https://doi.org/10.1057/jit.2015.5