Chapter 6

Online Privacy and Surveillance

> If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.
>
> Eric Schmidt

> The real danger is the gradual erosion of individual liberties through automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.
>
> US Privacy Study Commission (1977)

The House Is Watching, and Listening

James Andrew Bates was charged with murder in connection with the death of Victor Collins, who was found floating in Bates' hot tub in November 2015. In what may be the first case of its kind, police investigating the murder in Bentonville, Arkansas, issued a warrant to Amazon to turn over audio and other recordings from an Echo device in the suspect's home. Prosecutors believed Bates' Echo – a smart speaker device that connects to the Amazon voice-activated personal assistant Alexa – may have been a key 'witness' to the crime and obtained search warrants for all the device's recordings.[1] Since Alexa, and other digital voice-activated assistants, listen out at all times for pre-recorded 'wake up words', police anticipated that audio recordings of the moments and events leading up to the suspected murder were captured by the device. Police also used other Internet

[1]Dotan, T., & Albergotti, R. (2016). Amazon Echo and the hot tub murder. *The Information*, December 27. Retrieved from https://www.theinformation.com/articles/amazon-echo-and-the-hot-tub-murder

The Social, Cultural and Environmental Costs of Hyper-Connectivity: Sleeping Through the Revolution, 85–102

doi:10.1108/978-1-83909-976-220211006

of Things devices to gather evidence in the case. A connected water meter, for instance, showed that a significant amount of water was used between 1 a.m. and 3 a.m. the morning of the alleged crime which, police claimed, Bates used to hose down his patio and hot tub in order to hide vital evidence. Amazon twice declined to provide the authorities with the relevant recordings and information they requested, although they did provide Bates' account information and purchase history. The company argued that both its users' requests to Alexa and its own responses were protected by US First Amendment Rights, and that law enforcement agencies must meet a much high burden of proof to require release of such personal data. The impasse was broken when Bates himself agreed to allow the police review the information contained on his Echo, which prompted Amazon to hand over the data thus dropping its legal challenges. While the battle over the personal data from the Amazon Echo device had been resolved in this particular case, the question of whether our personal information, recorded and stored by such devices, is actually secure and protected has not been truly answered. Other recent high-profile contests over the collection and storage of personal data, and who has the rights to access to such information, include the Federal Bureau of Investigations' (FBI) request to Apple for the data from two iPhones that belonged to the gunman in the shooting at a naval base in Pensacola, Florida,[2] and the US Department of Justice's request for email data stored by Microsoft as part of a drug-trafficking investigation.[3] The possibility of eaves-dropping on individuals and groups, and the storage of such private conversations by internet-connected devices in the home, raises additional serious concerns and issues over privacy and surveillances, even unintentionally, in this new digital age. Legal challenges will, no doubt, develop again as part of future criminal investigations and government agency requests, opening yet other fronts in the tug-of-war between big tech companies and law enforcement and government agencies over our personal data privacy. More troubling may be the stark realisation that these household devices are listening and collecting our private data at all times of the day and night.

Privacy in the Digital Age

Debates about online privacy and surveillances have echoes of those on freedom of speech and censorship, which have been ongoing for centuries. These deliberations have become some of the fundamental challenges of the information age and although not new, this is now the latest iteration of an age-old battle over the control and dissemination of information. In a modern context, how much about an individual's life and actions are the people around them entitled to know, and

[2]Nicas, J., & Benner, K. (2020). F.B.I. asks Apple to help unlock two iPhones. *The New York Times*, January 7. Retrieved from https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html

[3]Matsakis, L. (2018). Microsoft's Supreme Court case has big implications for data. *Wired*, February 27. Retrieved from https://www.wired.com/story/us-vs-microsoft-supreme-court-case-data/

what restrictions and limitations should be placed upon mammoth online digital platforms and corporations over the industrialised collection and control of such personal information? An individual's freedom to protest when they feel something needs changing, to freely associate with others, to move around their own country without hindrance, to read and to write without wondering who is tracking their every movements and motives; these are all universally recognised fundamental rights in democratic societies. Debates and discussions that have been ongoing since the birth of nations have led many countries to pass strict laws protecting personal data against particular types of mismanagement and misuse. But personal data protection in the digital age is one of those issues where an understanding of the ramifications, consequences and implications largely depends on a comprehensive awareness of the fundamental issues involved: be they personal, social, political or cultural.[4] More importantly, in a globalised, borderless digital world, many of the national and international laws protecting privacy have failed to keep pace with the realities of online communications and digital technology development.

The initial underpinning philosophy of the World Wide Web was that of a free and open network: free in the context of unrestricted, while open signified a lack of barriers or controls to access or use. Having both concepts meant anyone and everyone could log on, wherever and whenever they choose to do so, search any website they wished and download any file they need, all without any third parties' interference shaping their online interactions and experiences. Censorship was arguably the biggest threat to this early iteration of a free and open internet. But the following iteration of the Web saw a profound change in the philosophy and in the approaches of Web companies, Web developers and, more importantly, a change in the expectations and values of a Web-savvy society as a whole. Web 2.0 marked a turning point for the network in that individuals were no longer just using the internet as a tool or broadcast medium, users were now becoming a part of it and merging with the network itself. Not only were we using the internet more and more, but we were also using it differently. Suddenly, Web-savvy users could input an extensive amount of information into forms and Web fields and send this back to the servers, so that they were effectively communicating with hosting servers in real time. It was described as a move towards a more social, collaborative, interactive and responsive Web in which we were not just passively consuming content but instead also adding to the collective knowledge of the network. It shifted from a read-only internet to a read/write network, with an emphasis on social networking, content generated by ordinary users, and cloud computing.

It is interesting that in this transition to Web 2.0, we had begun to unconsciously and generously given away much of our privacy without any real consideration of the impacts or consequences of such actions. It's often the price we are willing to pay for using free services provided by social networking platforms and online megacorporations. But is there ever a free lunch, and just how high a price are we paying? For many social media users, surveillance – and especially surveillance-as-control – does not appear important to them, and it seems that for

[4]Adam and McCrindle (2008).

many control is in their hands as they choose whom to accept or deny as friends and build their networks of like-minded acquaintances. But for all the benefits that accrue to those supported to stay connected with their social media contacts, each click permits more and more personal data to be accumulated, and as this pool of personal data builds, there is less and less accountability about how it is used.[5] The consequences of this are considerable. Data have now surpassed oil as the most important and tradable commodity on earth, and big tech is leading the charge to cash in on all our personal information. To begin, we need to look at the more recent context of privacy in the information age, and the compromises that have been made over the years, before we move to present the problems for privacy presented by digital information and communication (ICT) technology and social media platforms in the twenty-first century.

Privacy Matters

Definitions of privacy have always been broadly based on information in all its various forms. It is said to be a value that needs to be understood as an aspect of autonomy for individuals containing both freedom from undue demands to conform and freedom to control one's own personal information.[6] Successive interpretations are iterative in their development and have moved from suggesting that just paper and correspondence should be protected from invasion intent, to now include communications in all its forms as well as ones private life.[7] The general concept of privacy uses the theory of natural rights and has now attempted to respond to new forms of digital ICT. While an internationally binding agreement on the protection of privacy does not exist, the right to privacy is explicitly stated under Article 12 of the 1948 *Universal Declaration of Human Rights*:

> No one shall be subjected to arbitrary or unlawful interference with his privacy, home or correspondence, nor to unlawful attacks on his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.[8]

There have been various other Human Rights declarations since the initial document,[9] and all have, in some way, included aspects of the right to privacy

[5]Trottier and Lyon (2012, p. 92).
[6]Cheung (2009, p. 209).
[7]Adam and McCrindle (2008, p. 215).
[8]Universal Declaration of Human Rights. (1948). *The United Nations*, December 10. Retrieved from https://www.un.org/en/universal-declaration-human-rights/index.html
[9]Article 17 of the *International Covenant on Civil and Political Rights* (United Nations, 1966), Article 8 of the *European Convention of Human Rights* (Council of Europe, 1950) and Article 7 of the *Charter of Fundamental Rights of the European Union* (2000) state that the right to privacy is a fundamental human right and everyone has the right for their private and family life, home and correspondence to be respected, and they have the right to protect themselves against such unlawful interference.

as a first-generation fundamental human right. Privacy protection would often subsequently appear in national legislation in countries adopting these declarations. By the 1960s, many homes in the developed world were acquiring telephones and televisions of their own, and at the same time, the Cold War was intensifying and beginning to dominate the narrative of many nations. In this era of rising suspicion, invasive surveillance was normalised as something patriotic to counteract the aggression of the other side, but much of this was primitive in nature and relied heavily on a paper-based collection and storage of information. With the collapse of the Soviet Union in the late 1980s, the need for such large-scale surveillance weaned somewhat. This is not to say that the harvesting of personal information stopped. The use of personal data has always been a fundamental part of marketing and advertising, and individual states and countries have also used their census of household information, and other data sources, in attempts to predict long-term trends and assist with policy creation and design. It's just that the new emerging networked and information society, in the form of digital computing, was now allowing the collection and storage of such data to become much easier and on a mass scale. More significantly, the mining of these data for new meaning and understanding was now possible leading to fresh opportunities for marketing and advertising agencies, but also new threats and dangers to our personal data and information with the potential for manipulation of such data growing on a vast scale.

By the 1990s, two separate approaches to data protection and privacy regulation began to emerge in the Western world: in the United States and Europe, respectively. These two strands fundamentally differ in that the American approach is focussed on self-regulation and free market forces, while the European approach is one of government regulation and stricter laws. While these two threads of data protection and privacy regulation continued to develop over the decades that followed, they present some enduring difficulties for international trade which interfaces between the two regions. By 1995, common European minimum standards on data protection were agreed,[10] which was an important first step in the development of a European-wide single market. Once implemented, these standards allowed for the free movement of personal information between European countries – after appropriate protection had been enshrined in each country – and also allowed for the limited transfer of certain data outside of the European Union (EU). The General Data Protection Regulation (GDPR),[11] adopted in April 2016, superseded the Data Protection Directive and became enforceable on 25 May 2018. The principle aim of GDPR is to give control back to individuals over their own personal data and to simplify the regulatory

[10]Data Protection Directive 95/46/EC. *The European Parliament and Council*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046

[11]General Data Protection Regulation (GDPR). *The European Parliament and Council of the European Union*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

environment for international business by unifying the rules within the EU and the European Economic Area (EEA). Companies and organisations who wish to operate within the EU now must clearly ask individuals for their permission to use their personal data. They can no longer just use what they have collected and tell individuals after the fact. If they do, then penalties will apply based on the company's size and the extent of misuse. These new regulations gave rise to much debate and controversy with many businesses reporting that compliance with GDPR would require additional heavy investment in their data management systems.[12] Other businesses supported the measures suggesting that it would lead to an improvement in organisational data management, and consumer rights groups and advocates were among the most vocal proponents of the new legislation. In effect, this new regulatory environment has shifted power over personal data away from corporations and back to the individual.

Meanwhile, the US approach to privacy and personal data protection had taken a different route than that of Europe. The United States lacks a single comprehensive federal law that regulates the collection and use of personal data; instead the government has approached privacy and data security by regulating only certain sectors and types of sensitive information – health and financial data – creating overlapping and contradictory protections.[13] In keeping with the conventional market-driven approach that exists in the country, the Federal Trade Commission (FTC) merely issues general guidelines about appropriate privacy policies and enforces adherence to organisational published policies.[14] The rational underpinning this approach is that if privacy and data protection is important to the individual, then they will opt to interact or seek the services of companies and organisations that offer the best protection and control. This will, in turn, force organisations into better control and data management, and the regulatory role of the FTC comes into play only to prevent companies from publishing one policy but covertly using a separate one in an attempt to gain competitive or market advantage. This light touch regulatory approach is strongly market focussed and is heavily dependent on company respect for such personal data, and overall corporate responsibility and integrity.

The fundamental difference between the US and EU approaches when it comes to data protection is their point of focus. The United States is concerned with the integrity of data as a commercial asset. GDPR in Europe has firmly put individual rights before the interest of businesses. Both strands appear to be ideologically opposed, and countermoves against each are being implemented and used. For example, The US Department of Commerce created the *International*

---

[12]Babel, C. (2017). The high costs of GDPR compliance. *Dark Reading*, July 11. Retrieved from https://www.darkreading.com/endpoint/the-high-costs-of-gdpr-compliance/a/d-id/1329263?

[13]Connor, N. O. (2018). Reforming the U.S. approach to data protection and privacy. *Council for Foreign Relations*, January 30. Retrieved from https://www.cfr.org/report/reforming-us-approach-data-protection

[14]Adam and McCrindle (2008, p. 227).

Safe Harbor Privacy Principles certification programme in response to the earlier 1995 European Directive on Data Protection. The principle behind Safe Harbor was to prevent private organisations within the EU or United States who store customer data from accidentally disclosing or losing such personal information.[15] Companies in the United States collecting and storing customer data are to self-certify that they adhered to seven principles to comply with the EU Data Protection Directive, and the European Commission made a decision in 2000 that these principles did comply with the EU Directive. However, after a customer complained that his Facebook data were insufficiently protected, the European Court of Justice declared in October 2015 that its earlier decision was invalid,[16] leading to further talks being held by the Commission with the US authorities towards a renewed framework for transatlantic data flows. While the contest between the two approaches to privacy and data protection plays out, the big tech companies who gather and amass large volumes of personal data in both jurisdictions retain their distinct advantage in that these data can be moved quickly and effortlessly between Europe and the United States when the need arises.

Ground Zero for the Digital Surveillance

One of the most significant shocks to policy and public opinion with respect to privacy and surveillance occurred at the very beginning of the new millennium. The terrorist attacks on the World Trade Centres in New York and on the Pentagon in Washington on 11 September 2001 marked a significant shift in the political direction of many liberal democracies across the world, leading to an undeniable shift in attitude towards freedom of speech, surveillance and the security of personal data. Some major policy changes followed as the threat from acts perpetrated from within their own country became a reality for most Americans. The newly created US Department of Homeland Security, together with intelligence agencies such as the Central Intelligence Agency (CIA), National Security Agency (NSA) and FBI, began placing a higher value on surveillance of electronic and digital communications. This followed some significant criticism of failings within the FBI and CIA to apply and use available information prior to the attacks, including about some of the terrorists the CIA knew were in the United States.[17] Against the backdrop of the attacks in New York and Washington, there was little opposition from most political leaders and parties to radical steps being taken that would tip the balance towards mass surveillance of all citizens' right across society and away from individual freedoms and privacy. This allowed for the passing of the Patriot Act into US law and the Terrorism

[15]A brief introduction to the Safe Harbor agreement. *Agreements.org*. Retrieved from https://www.agreements.org/safe-harbor-agreement.html/

[16]The Court of Justice declares that the Commission's US Safe Harbour decision is invalid. (2016). *Court of Justice of the European Union*, October 6. Retrieved from https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

[17]Immerman (2006).

Crime and Security Act 2001 into UK law with little political debate, discussion or opposition. The Patriot Act expanded the abilities of law enforcement to use mass surveillance – including the tapping of domestic and international phones – it eased interagency communication to allow federal agencies to effectively use all available resources in counterterrorism efforts and increased penalties for terrorism crimes and an expanded list of activities which would qualify someone to be charged with terrorism.[18] The Terrorism Crime and Security Act 2001, in part, established wide powers for the Secretary of State to regulate telephone companies and internet providers to retain data for the purpose of national security.[19] Civil rights groups were critical of both acts suggesting they had little to do with combating terrorism and instead contained measures that could be used to advance authoritarian power and for use in other law enforcement activities rather than defeating terrorism. David Cole, Professor of Law at Georgetown University, explained in a July 2003 interview with Bryant Gumbel:

> [The Patriot Act] gives the government the ability to spy on its citizens and on foreign nationals without probable cause of a crime, to get wiretaps and warrants. It gives them the ability to get records from libraries and book stores on people who are not targets of any criminal investigation, who are not targets of any foreign intelligence investigation and who are not suspected of engaging in any illegal activity … But it's one thing to make some sacrifices in terms of privacy but another thing to throw the fourth amendment out the window.[20]

Some two decades later, it would be naive to think that democratic governments have stopped covertly collecting our personal data on a mass scale as the international terrorist threat recedes. In a study for The Pew Research Center in 2019, a majority of Americans believed their online and offline activities were being tracked and monitored by their government, and online and offline companies and organisations, with some regularity.[21] Nearly two thirds reported being concerned about the way their data were being used by their government. It is such a common condition of modern life that roughly six in 10 US adults say they

---

[18]Pub.L.107-56. *uslaw.link*. Retrieved from https://uslaw.link/citation/us-law/public/107/56

[19]Most of the measures in the act were not specifically related to terrorism, and a parliamentary committee was critical of the swift timetable for such a long bill to pass. The Act was widely criticised, and on 16 December 2004, the Law Lords ruled that Section 23 was incompatible with the European Convention on Human Rights, but under the terms of the Human Rights Act 1998, it remained in force. It has since been replaced by the Prevention of Terrorism Act 2005.

[20]Patriot Act Debate Transcript. (2003). *Flashpoint USA*, July 15. Retrieved from https://www.pbs.org/flashpointsusa/20030715/infocus/topic_03/trans_pat_act.html

[21]Auxier et al. (2019).

do not think it is possible to go through daily life without having their personal data being collected and analysed by big tech or the government. But even as the public expresses anxiety about various aspects of their digital privacy, many acknowledge that they are not always diligent about paying attention to the privacy policies and terms of service they regularly encounter surfing the internet. Fully 97 per cent of Americans say they are regularly asked to approve privacy policies, yet only about one-in-five adults say they always or often read a company's privacy policy before agreeing to it. If we care so much about protecting our personal information and feel uncomfortable about giving it away so freely why then do we keep doing it, and why do not we do anything about it later? Researchers call this conundrum the 'privacy paradox'.[22] We freely divulge personal information in exchange for services and convenience and in the case of government agencies to remain active citizens. Our governments are ultimately accountable to their citizens, and the prospect of inappropriate surveillance or the misuse of personal data will, we hope, be uncovered by the media or whistle-blowers and punished in the courts or at election time. But what about other regimes who operate to different standards and who use these digital surveillance technologies for more sinister purposes?

Digital Surveillance States

China's internet censorship is perhaps the most sophisticated and advanced than that in any other country in the world. The state is continually ramping up its ability to spy on its nearly 1.4 billion people to new and disturbing levels, giving the world a blueprint for how to build a digital totalitarian state. Chinese authorities have knitted together old and state-of-the-art technologies, such as paper-based files, phone scanners, facial recognition software and cameras, face and fingerprint databases and many others instruments of surveillance, into a comprehensive toolkit for authoritarian control, according to police and private databases examined by *The New York Times*.[23] Once assembled and fully operational, this digital technology toolset for repression will help police and authorities determine the identity of people as they merely walk down the street, finding out who they are meeting with and identify those who belong, and do not belong, to the ruling Communist Party. Such a surveillance apparatus gives authorities the potent means to track criminals as well as online dissidents and malcontents, sympathisers of the protest movement in Hong Kong, critics of

[22]For a good explanation of the privacy paradox: see Bongiovanni, I., Renaud, K., & Aleisa, N. (2020). The privacy paradox: We claim we care about our data, so why don't our actions match? *The Conversation*, July 29. Retrieved from https://theconversation.com/the-privacy-paradox-we-claim-we-care-about-our-data-so-why-dont-our-actions-match-143354

[23]Mozur, P., & Krolik, A. (2019). A surveillance net blankets China cities, giving police vast powers. *The New York Times*, December 17. Retrieved from https://www.nytimes.com/2019/12/17/technology/china-surveillance.html

police actions and that of the authorities and other undesirables as determined by the state. This immense digital surveillance system also regularly targets vulnerable groups like migrant workers and ethnic minorities such as the largely Muslim Uighurs on China's western frontier. Surveillance technologies are being used extensively to support the continuing clampdown in Xinjiang, in which the state have corralled as many as a million ethnic Uighurs, Kazakhs and others into 're-education' internment camps or prisons over the past three years. Beijing has sought for decades to suppress Uighur resistance to Chinese rule in Xinjiang, and according to leaked internal documents, ensuring stability in Xinjiang will require a sweeping campaign of surveillance and intelligence gathering to root out resistance from within Uighur society.[24] President Xi Jinping has maintained that new digital technology will play a key role in quashing resistance, foreshadowing the party's deployment of facial recognition, genetic testing and big data in Xinjiang. But he also emphasised old-fashioned methods such as neighbourhood informants and, ironically, urged officials to study how America responded to the September 11 attacks.

Internet content in China is tightly controlled, closely monitored and micromanaged by the Communist Party, and in recent years, the leadership has devoted more and more resources to controlling all forms of online content. Known as 'The Great Firewall of China', the one-party state not only sets up official agencies to monitor online information and content but also uses legal means to require internet content providers to build their own self-censorship mechanisms.[25] Research also indicates that the Chinese government fabricates social media profiles and posts for positive propaganda and opinion manipulation.[26] In the virtual world, as in the real world, the ruling party has moved to silence dissenting voices, to mobilise party members in support of its preferred values and to prevent foreign ideas from seeping into Chinese political, cultural and social life. The vast collection and use of big data gleamed from the digital world has also allowed the state to create a 'social credits system' scoring citizens on their personal conduct and measuring their sincerity, honesty and integrity.[27] Such scoring is a major determinant for whether individuals or families can get credit; rent a flat; buy a plane ticket; and get access to a hospital, university or government services. In a leaked speech in August 2013, Chinese president Xi Jinping

[24]Ramzy, A., & Buckley, C. (2019). Absolutely no mercy: Leaked files expose how China organized mass detentions of Muslims. *The New York Time*s, November 16. Retrieved from https://www.nytimes.com/interactive/2019/11/16/world/asia/china-xinjiang-documents.html

[25]Ng, J. Q. (2012). How China gets the internet to censor itself. *WagingNonviolence*, March 12. Retrieved from https://wagingnonviolence.org/2012/03/how-china-gets-the-internet-to-censor-itself/

[26]Meyer, D. (2016). Here's how the Chinese government really manipulates social media. *Fortune*, May 20. Retrieved from https://fortune.com/2016/05/20/chinese-social-manipulation/

[27]Mac Síthigh and Siems (2019).

articulated the belief that a shift is now taking place, and 'the internet has become the main battlefield for the public opinion struggle'.[28]

China is far from alone in its efforts to amass and control the copious flow of online data and information and in deciding the narrative of acceptable social and political discourse. In the face of the Covid-19 coronavirus global pandemic, some countries, such as Taiwan and Singapore, took deceive action to contain the spread of the virus using big data, CCTV, smartphone apps and widespread surveillance mechanisms. While it is hoped that such measures will be rolled back as the pandemic dissipates, in other countries, these surveillance measures may well become the norm and new reality for citizens. The Moscow correspondent for *The Guardian*, Andrew Roth, reported that the Russian authorities were considering aggressive new surveillance methods as the country seeks to enforce mandatory shelter-in-place orders in cities including Moscow and St Petersburg and other regions across its 11 time zones.[29] While the details of this new monitoring system were not confirmed, official statements and leaked plans indicated that measures would include mobile apps that track users' location, CCTV cameras with facial recognition software, QR codes, tracking mobile phone data and credit card records. This is not a new development but part of ongoing efforts to transform that country into a mass surveillance state. For years, Russian secret services have been busy tightening their hold over internet content and users and have begun helping their counterparts in the rest of the former Soviet Union to do the same, according to investigative journalists working for World Policy.[30] Russia is attempting to splinter the Web, breaking off from the global internet a Russian intranet that will be much easier for it to control and manipulate. The reason for such control is obvious. The old forms of surveillance used by the KGB before the fall of the Soviet Union were expensive and cumbersome and involved the physical tapping of telephones and the covert following and documentation of the movements and interactions of people of interest. The shift in communications to the digital realm effectively solves many of the problems that plagued surveillance in the analogue age. It is cheaper, storage space is almost infinite, equipment reasonably cheap and such digital technology allows for doing more with less resources.

---

[28]Economy, E. C. (2018). The great firewall of China: Xi Jinping's internet shutdown. *The Guardian*, June 29. Retrieved from https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

[29]Roth, A. (2020). Cybergulag: Russia looks to surveillance technology to enforce lockdown. *The Guardian*, April 2. Retrieved from https://www.theguardian.com/world/2020/apr/02/cybergulag-russia-looks-to-surveillance-technology-to-enforce-lockdown

[30]Andrei Soldatov and Irina Borogan are Russian investigative journalists who cover the operations of Russian security services. They are co-founders of the website Agentura, which chronicles the services' activities. They also co-authored *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (Public Affairs, 2011).

Russia and other authoritarian regimes are not novices when it comes to such clandestine and shadowy use of digital ICT, and some lone voices have been warning us about the ever-increasing sophistication of their cyber capabilities long before we actually witnessed their interference into the democracy processes in both the United States, with the election of Donald Trump, and the Brexit vote in the UK. In *The Net Delusion*, published in 2011, Evgeny Morozov maintains that the internet is helping authoritarian regimes in China, Russia and Iran to strengthen their grips on those countries.[31] These oppressive governments are using cyberspace to stifle dissent, plant clandestine propaganda, employing sophisticated digital censorship and using online surveillance on a mass scale. The success they have achieved with their approaches to digital censorship, surveillance and oppression at home has emboldened these regimes to expand their cyber capabilities to interfere and disrupt the democratic processes in many Western societies, and this has been allowed to happen because of our naivety towards the purpose and intention of all digital ICT. There was previously widespread belief that such authoritarian governments and their security apparatus were too backward and technophobic to use digital surveillance and other similar cyber tricks to control their people and spread dissent and confusion in the democratic world. We have awoken to this possibility with somewhat of a shudder. We had been promised an internet that would liberate the world; instead we are awakening to a much opaquer digital online world frequently controlled by dark forces we cannot see or control. Research and understanding is now urgently needed into the functioning of surveillance software to address the problem of who will know, and in that way, we can bear witness to programmes that 'social-sort' or that threaten difference, while keeping tabs on what and how much personal information is collected and by whom.[32]

The Cambridge Analytica Scandal

But it is not only the use of digital surveillance and data manipulation by national governments that we should be worried about. More troubling is the mismanagement and misuse of our private and personal data and information that we carelessly and liberally give away when we interact on social media platforms and surf the internet. Numerous academic studies have confirmed that every time we share our personal information on a social networking platform, we make it more likely that someone, or organisation, might use it to predict what our likes or dislikes are, and knowing what our preferences are is always a good first step towards controlling our behaviour.[33] The personal information we share on social networking platforms, with friends and family, has been monetised and weaponised and repackaged in attempts to gradually and steadfastly change our behaviours over time. The most recent example of this to be exposed has been the

[31]Morozov (2011).
[32]Hill (2012, p. 121).
[33]For a good understanding of how our social networks, in general, affect our lives (Christakis & Fowler, 2009).

Cambridge Analytica scandal, a year-long investigation into Facebook, personal data and the influencing of voting behaviour in the digital age. The discovery that Facebook had given unfettered access to the personally identifiable information of more than 50 million unsuspecting Facebook users[34] to the data firm Cambridge Analytica added to the growing concern over digital ICT's societal roles and impacts and the risk to citizen's privacy and well-being. The scandal broke as a result of a year's work by investigative journalism Carole Cadwalladr for *The Observer* newspaper, who then took the decision to share the revelations with *The New York Times* and with Channel 4 News to pool their investigative resources and broaden the reach of their investigation.[35] Alexander Nix, the chief executive of Cambridge Analytica, and his managing director Mark Turnbull, were exposed explaining to undercover Channel 4 reporters how they had manipulated the voters of democracies across the globe – most notably in Britain and the United States – with unsourced and misleading propaganda, and also boasting of sting operations and honey traps in some countries. They were able to do much of this by means of the mismanagement and misuse of private and personal data gleamed almost effortlessly from Facebook.

This story began in 2013 when researchers at the University of Cambridge's Psychometrics Centre began analysing a series of personality tests, available to Facebook users, to evaluate if their psychological profile correlated in any way with a person's actual Facebook activities such as their 'likes' or 'shares'. This particular body of research drew in some 350,000 US participants and established a clear relationship between the individual's Facebook activity and this five-factor psychological personality profile,[36] but there was no evidence that this particular body of research had exposed participants to any specific privacy abuse. In fact, it is widely claimed that the university refused to share either individual's personal data or the resulting criteria with what would later become Cambridge Analytica.[37] While working on the original Cambridge University research, academic Aleksandr Kogan had separately developed an app called *thisisyourdigitallife*, which was designed to collect similar personal data from Facebook users. Through his own company Global Science Research (GSR), and in collaboration with Cambridge Analytica, hundreds of thousands of users were paid to take the personality test and agreed to have their data collected and analysed for academic purposes. However, the app also collected the personal data of the test-takers' Facebook friends list, leading to the illicit accumulation of a data pool tens of millions strong. All the while Facebook were ignorant to such an unprecedented personal data breach and negligent in their duty of care to the entire Facebook community.

---

[34]Facebook themselves later revised this figure upwards to a staggering 87 million users.
[35]*The Observer's* investigation and full story of the scandal is available in 'The Cambridge Analytica files' at https://www.theguardian.com/news/series/cambridge-analytica-files.
[36]The five-factor profile included openness, conscientiousness, extraversion, agreeableness and neuroticism.
[37]Isaak and Hanna (2018, p. 57).

Cambridge Analytica were quick to realise they could integrate this dishonestly acquired Facebook information with a range of other data from other social media platforms, Web browsers, online purchases, voting patterns and results and other such available data. By correlating this with the five-factor psychological personality profile, they developed the ability to then micro-target individual customers and voters with messages most likely to influence their behaviour.[38] Using these psychographic profiles – as the company calls them – Cambridge Analytica not only identified which voters were most likely to shift to their causes or candidates; they could use this information to predict and then change future behaviours.[39] It was an attempt at social engineering not witnessed heretofore, made possible but an extraordinary breach of personal data and the application of digital technology and algorithms. The company boasted that they had been instrumental in both the election of Donald Trump in the United States and the successful leave campaign in the Brexit referendum and became subject to investigations on both sides of the Atlantic. The company was a key organisation of interest in two inquiries in the UK – the Electoral Commission into the firm's possible role in the EU referendum and the Information Commissioner's Office into data analytics for political purposes – and one in the United States: part of special counsel Robert Mueller's probe into Trump-Russia collusion.

The scandal exposed the misuse of personal data on an enormous scale. It was an attempt to influence people, auctioned off to the highest bidder and regardless of the morality and ethics of the purchaser or their cause or the consequences for wider society. While Cambridge Analytica became the scapegoat and must take its fair share of the blame for what only can be described as its shadowy wrongdoings, a higher proportion of the blame must be apportioned to Facebook. Their negligence in failing to protect user's personal information leading to a large-scale breach of trust, and their overall mismanagement of personal data on a colossal scale, stands testimony to an organisation that is unrestrained and unpunished in their misconduct and unrepentant when caught out. Facebook's initial reaction to the scandal was an attempt to silence the journalists and media outlets involved in the investigation warning *The Observer* that it 'was making false and defamatory allegations, and reserved Facebook's legal position'.[40] But it's not only Facebook that is cashing in and failing to protect personal data. The Cambridge Analytica claim to have over 5,000 data points from which to draw

[38]In a presentation at the 2016 Concordia Annual Summit in New York, Alexander Nix outlined how big data and psychographics work in reality: see https://www.youtube.com/watch?v=n8Dd5aVXLCc.

[39]Anderson, B., & Horvath, B. (2017). The rise of the weaponized AI propaganda machine. *Scout*, February 15. Retrieved from https://www.scout.ai/story/the-rise-of-the-weaponized-ai-propaganda-machine

[40]Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, March 17. Retrieved from https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

upon to build their psychological profiles of individual voters remains a deeply disturbing aspect of this scandal. The techniques used by Cambridge Analytica may also have emboldened others to seek similar control and leverage with regard to the use of personal data and surveillance.

A recent report from the Carnegie Endowment for International Peace suggests that almost half the world's nation states now deploy artificial intelligence (AI) surveillance systems to monitor, track and spy on their citizens to accomplish a range of policy objectives – some lawful, others that violate human rights and many of which fall into a murky middle ground.[41] In presenting an AI Global Surveillance (AIGS) Index, which represents one of the first research efforts of its kind, the report maintains that at least 75 out of 176 countries investigated are now actively using digital surveillance, and that these technologies are spreading at a faster rate to a wider range of countries than experts have previously assumed. China was reported to be the major driver of AI surveillance worldwide, and digital technology linked to Chinese companies such as Huawei, Hikvision, Dahua and ZTE are suppling AI surveillance technology to 63 countries, 36 of which have signed up to the China's Belt and Road Initiative (BRI). The Chinese product pitches are often accompanied by soft loans to encourage governments to purchase their equipment. These tactics are particularly relevant in countries like Kenya, Laos, Mongolia, Uganda and Uzbekistan, which otherwise might not have the resources or access to such technology. But this raises troubling questions about the extent to which the Chinese government is subsidising the purchase of advanced repressive technology, and their role and sphere of influence within these countries.

While authoritarian states are continuing to invest heavily in such digital surveillance equipment, worryingly the trend for its use in more democratic countries is also on the increase. There is also little evidence of any adequate steps to monitor and control the use and spread of such sophisticated technologies linked to a range of violations of our personal data and privacy. While this does not inevitably mean that liberal democracies are abusing these systems, such governments are 'aggressively using AI tools to police borders, apprehend potential criminals, monitor citizens for bad behaviour, and pull out suspected terrorists from crowds'.[42] And what of the link between governments and big tech, and how is such cooperation impacting our rights to privacy? Such global surveillance modification systems are threatening human nature itself, and this is the central thesis of Shoshana Zuboff's provocative 2019 book *The Age of Surveillance Capitalism*.[43] In this text, she argues that just as industrial capitalism had disfigured the natural world in the twentieth century, now a surveillance capitalism advances from Silicon Valley into almost every sector of the global economy creating vast wealth and power for those attempting to predict our behaviour:

[41]Feldstein (2019).
[42]Feldstein (2019, p. 10).
[43]Zuboff (2019).

> Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioural data. Although some of these data are applied to product or service improvement, the rest are declared as a proprietary *behavioural surplus*, fed into advanced manufacturing processes known as 'machine intelligence', and fabricated into *prediction products* that anticipate what you will do now, soon, and later. Finally, these predications products are traded in a new kind of marketplace for behavioural predictions that I call *behavioural futures markets*. Surveillance capitalists have grown immensely wealthy from these trading operations, for many companies are eager to lay bets on our future behaviour.[44]

All the major digital tech conglomerates are involved at various levels. Google have been the pioneers of surveillance capitalism and were trailblazers in terms of experimentation and implementation, with its deep pockets for research and development. But the business model quickly spread to Facebook and later to Microsoft, and there is now strong evidence that Amazon are using many of these approaches and practices on their platforms. Zuboff argues that what starts with predication ends with control. These platforms have moved beyond merely strip mining our deepest and most personal thoughts and information and are now seeking to shape, direct and control our present and future behaviour. Ignorance of its operation is one of the central strategies of this regime, and surveillance capitalism, she suggests, is as profoundly undemocratic as it is exploitative, yet remains poorly understood. Surveillance capitalism continues to evolve and has moved from a focus on the individual users to a focus on populations and society itself, and all the while democracy slept as these digital mega-platforms amass unprecedented concentrations of knowledge and power based on personal information gleamed from their widely used platforms and services.[45]

Who Protects Our Privacy?

The lessons from surveillance capitalism and the Cambridge Analytica scandal are clear. We must be much more vigilant and more aware of the substance and amount of personal data we freely give away to online social media corporations and treat such platforms as broadcast medium where we should not post anything we would not shout out in a crowded room. But there is always information we post that we expect to be kept secure and not used by any third party. We also, therefore, need to be more vigilant with our own security settings and seek to protect our personal data in whatever way we possibly can. These online digital

---

[44] Zuboff (2019, p. 8).

[45] John Naughton interviews Shoshana Zuboff. (2019). The goal is to automate us: Welcome to the age of surveillance capitalism. *The Guardian*, January 20. Retrieved from https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

technology goliaths cannot be trusted to do the right thing with our personal data. But there will still be people who do not see the danger of thoughtlessly giving away their most intimate thoughts and feelings in order to avail of the free services big tech offers, and some might even say; so what! But none of us like to be duped into doing or thinking something based on our personal interactions that have been aggregated, manipulated, monetised and weaponised and used by shadowy forces to influence us in a particular way which often is working against our better interests and judgements. We all need to remain vigilant about how our personal data are used and be mindful to how privacy can be so easily encroached upon. Mark Zuckerberg reportedly spent $30 million on four surrounding houses to control how the properties around his home were marketed and who they were sold to.[46] The Facebook founder, who made his vast wealth on the use of our personal data, places a high value on his own privacy and space. Digital online corporations that owe their financial success and base their vast profits primarily on monetarising our personal data need much stronger oversight, regulation and control. Indeed, global challenges to our privacy brought about by digital networked ICT require strong internationally binding agreement to correct and rebalance the power and ownership over our personal data and information.

Digital-based surveillance and censorship continues to grow in scale, scope and sophistication around the world, and this growth is not surprising given the importance of many of these technologies in contemporary societies. But there is increasing cause for concern about the implications of these trends for media freedom, for unhampered discussion of matters of public interest and even for political activism in many states and regions. The coronavirus pandemic has also led to an unprecedented global surge in digital surveillance, researchers and privacy advocates around the world have warned, with billions of people now facing increased monitoring, something that may prove difficult to roll back over the coming years.[47] But maybe sometimes we cannot point the finger at these platform corporations when our privacy is compromised and instead must look more closely at the digital technology itself and our own behaviour. What we post may well have consequences well beyond what we expect. In Japan, in 2019, an obsessed fan hunted down his idol by zooming in on high-resolution photos of her eyes to discover clues to her whereabouts. Hibiki Sato, 26, was besotted with 21-year-old Japanese pop star Ena Matsuoka and assaulted her in September outside her front door inside an apartment block. Sato admitted to the attack after he was arrested and revealed he studied selfies that Matsuoka posted on social media to find clues as to where she lived. Specifically, he zoomed in on high-resolution images of her face and looked at the reflections in her eyes. He matched

[46]Riggs, E. (2013). Mark Zuckerberg spends $30 million on four homes to ensure privacy. *NBC News*, October 11. Retrieved from https://www.nbcnews.com/business-main/mark-zuckerberg-spends-30-million-four-homes-ensure-privacy-8C11379396

[47]The Russian Roskomsvoboda internet rights group released a global tracker called Pandemic Big Brother to chart violations of digital rights around the world as a result of concerns about the coronavirus pandemic: see https://pandemicbigbrother.online/en/.

what he saw to locations on Google Maps and eventually pieced together her home address. According to local media reports,[48] he was even able to approximate the storey Matsuoka lived on based on the windows and the angle of the sunlight in her eyes.

References

Adam, A. A., & McCrindle, R. J. (2008). *Pandora's box: Social and professional issues of the information age* (1st ed.). Chichester: John Wiley & Sons.

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and privacy: Concerned, confused and feeling lack of control over their personal information. *Pew Research Center, November* 15, 1063.

Cheung, A. S. (2009). Rethinking public privacy in the internet era: A study of virtual persecution by the internet crowd. *Journal of Media Law*, *1*(2), 191–217.

Christakis, N. A., & Fowler, J. H. (2009). *Connected: The surprising power of our social networks and how they shape our lives*. New York, NY: Little, Brown Spark.

Feldstein, S. (2019). The global expansion of AI surveillance. Retrieved from https://carnegieendowment.org/files/WP-Feldstein-AISurveillance_final1.pdf

Hill, D. W. (2012). Jean-Francois Lyotard and the inhumanity of internet surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 106–123). New York, NY: Routledge.

Immerman, R. H. (2006). *The Central Intelligence Agency: Security under scrutiny* (A. Theoharis, R. Immerman, L. Johnson, K. Olmsted, & J. Prados, Eds.). Westport, CT: Greenwood Publishing Group.

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer*, *51*(8), 56–59.

Mac Síthigh, D., & Siems, M. (2019). The Chinese social credit system: A model for other countries? *The Modern Law Review*, *82*(6), 1034–1071.

Morozov, E. (2011). *The Net Delusion: How not to liberate the world.* London: Allen Lane.

Trottier, D., & Lyon, D. (2012). Key features of social media surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (pp. 89–105). New York, NY: Routledge.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.

[48]Stalker found Japanese singer through reflection in her eyes. (2019). *BBC News Asia*, October 10. Retrieved from https://www.bbc.com/news/world-asia-50000234