Wendy M. Grossman
http://www.pelicancrossing.net

How did we get to now – building Covid19 app Digital Privacy catastrophy one tech brick at a time

Overview

The decade between 2010 and 2020 saw the convergence of three previously separate tracks - physical world monitoring, Internet technologies, and law/policy - to create a privacy disaster. There were still a few wins: Britain, as part of the EU, adopted the General Data Protection Regulation (2016), which enhanced citizens' data protection rights and granted regulators increased enforcement powers, and public pushback against care.data, a 2014 plan to allow commercial researchers access to NHS patient data, forced a rethink.

As 2020 began, long-running concerns about mass surveillance and the loss of privacy became overwhelmed by the need to contain the SARS-CoV-2 pandemic. While even dedicated privacy advocates generally accepted the immediate need for exceptions, concern remained that these intrusions might persist after the emergency ended.

The following tale of privacy in Britain between 2010 and 2020 falls into three parts: the state of play at the end of 2019, the pre-pandemic "normal"; a topic-by-topic breakdown of how privacy changed between 2010 and 2020; and the early response to the COVID-19 outbreak, which set the stage for vastly expanded surveillance - temporarily, one hopes.

The state of play at the end of 2019

By the end of 2019, smartphones equipped with wifi and GPS, coupled with other sensors spread through public spaces such as railway stations and airports, made it possible to track people through physical space, while widespread cameras and incoming automated facial recognition were threatening the anonymity urbanites used to take for granted. Simultaneously, the tracking technologies developed to spread ads across the web were expanded to connect users across devices and track them into the physical world. All of this was governed by a legal framework that permitted the security services to hack devices and retain huge amounts of communications data, the latter despite repeated strikedowns from the European Court of Justice.

Despite the best efforts of privacy advocates, it wasn't until the former NSA contractor Edward Snowden's 2013 release of thousands of documents showing the extent of government surveillance of the Internet that the public began to pay attention. Several prominent data breaches also raised awareness, as did the wave of cookie consent pop-ups spawned by the 2018 passage of the EU's General Data Protection Regulation.

Even so, the incursions into privacy mounted exponentially in the course of the 2010s, fuelled by the massive rise in mobile devices, the expansion of adtech to monetise every possible online cranny, and the data exploitation and monopolistic practices that made it possible for a handful of dominant technology companies to extract most of the available economic value.

One of the biggest shocks, in 2019, was the discovery that gambling companies had gained access to the data pertaining to the 28 million children in the Learning Record Service database via a third-party company the Department of Education authorised, apparently for the purpose of age verification. The breach included names, ages, and physical addresses.[1]

A second shock was the decision of several police forces to begin trialling automated facial recognition without consultation. Abruptly, beginning in late 2019, a van might roll up and scan everyone in a public area, looking for matches against a terrorist watch list. In one such trial run by the Metropolitan Police, a man who pulled his jumper over his face to evade the scanner was arrested and eventually fined £90 for swearing at the police officer who stopped him.[2]

Topic breakdown

AI

By 2020 artificial intelligence primarily took the form of machine learning - fancy pattern recognition, with decisions automated via algorithms - using techniques pioneered in the 1980s by scientists such as Geoff Hinton. What changed to enable this type of AI to become a reality for image recognition, language translation, search, and voice recognition was three things: vastly greater computing power, better understanding of how to weight factors inside neural networks, and the ready availability of large amounts of training data.

Adtech

What began with cookies (see Cookies) expanded into many other forms of uniquely identifying web users such as Flash cookies, browser fingerprinting, advertising IDs, and Canvas fingerprinting. By 2020, Google, Facebook, and others had perfected techniques for identifying users across devices and into the offline world so they could connect online ads to completed purchases. The colonisation of the web by advertisers is often dubbed "surveillance capitalism", a

[1] "Betting companies given access to UK gov't information on millions of children", by Charlie Osborne, ZdNet UK, 2020-01-20: https://www.zdnet.com/article/betting-companies-given-free-rein-with-data-of-28-million-children/.

[2] "Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested", by Lizzie Dearden, *The Independent*, 2019-01-31: https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html.

term coined by Shoshanna Zuboff.[3] The growing awareness of the power of third-party tracking and profiling led many web users to download and install ad blockers, posing a particular problem for publishers, whose print advertising revenues collapsed as the web grew and failed to replace the lost income from online advertising revenues and subscriptions. By 2019, more than two-thirds of all digital spending went to Google, Facebook, and Amazon.[4] The sums involved give some idea of the value of personal data. Between 2015 and 2019, Facebook increased its revenues per user from $1.90 in 2010 to $7.40 in 2015 to $41.40 in 2019 and become a $200 billion business based on centralising our personal lives on their servers and extracting progressively higher fees from advertisers for access to those audiences. By then, Facebook (2.23 billion monthly active users), WhatsApp (1.5 billion), Messenger (1.3 billion), and Instagram (1 billion) were four of the top six most popular social media sites[5] and 93% of marketers used Facebook advertising regularly.[6]

By 2019, partly because of affiliate advertising, the average smartphone held more than 100 third-party cookies that were collecting every search and every opened web address. GDPR made little difference, showing that good intentions do not make privacy legislation successful.

Algorithms

An algorithm is a set of steps - a process - for completing a task. The problem with algorithms is not that they exist but how they are used; no computer software would exist without them, and in many systems they are harmless. In systems where there is not necessarily a right answer such as who gets state benefits, whether someone might become a terrorist, or how to rate a teacher's performance, by 2020 algorithmic decision making had become a vector for creating and perpetuating unfairness. Because these algorithms are trained on historical data (see also AI), the results of years or decades of biased human decisions are embedded in the training data, biasing the resulting systems.[7] An example in the UK is Durham's Harm Assessment Risk Tool, which Durham Constabularty tested as a way of identifying the subset of criminal offenders who

[3] *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, by Shoshanna Zuboff, Public Affairs Books, 2019.

[4] "Almost 70% of digital ad spending going to Google, Facebook, Amazon, says analyst firm", by Greg Sterling, Marketing Land, 2019-06-17: https://marketingland.com/almost-70-of-digital-ad-spending-going-to-google-facebook-amazon-says-analyst-firm-262565.

[5] "The 10 most popular social media sites in 2020", Top Ten Reviews, 2020-04-28: Facebook (2.23 billion monthly active users), WhatsApp (1.5 billion), Messenger (1.3 billion), and Instagram (1 billion).

[6] "Facebook by the Numbers: Stats, Demographics & Fun Facts", Omnicore, 2020-04-22: https://www.omnicoreagency.com/facebook-statistics/.

[7] *Weapons of Math Destruction*, by Cathy O'Neil, Crown Random House, 2016: https://weaponsofmathdestructionbook.com/.

are at moderate (not low, who are released, nor high, who are imprisoned) risk of committing further offenders and divert them to alternative interventions.[8]

Anonymisation

When organisations such as the National Health Service or the telephone companies want to exploit user data, they often rely on the claim that the data is "anonymised". However, over the last 20 years research has repeatedly shown that the claim to be able to anonymise data is unfounded. In 2000, for example, Sweeney showed that 87% of the US population could be uniquely identified by just their five-digit zip code, gender, and data of birth[9]; 99.98% can be reidentified using 15 characteristics from an anonymised dataset, including age, gender, and marital status - and companies like Facebook, Google, or Experian have over 100 data points on each individual.[10] Subsequent work by Sweeney and others has repeatedly shown that the increased availability of large datasets that can be cross-matched makes true anonymisation effectively impossible. The risk of reidentification has, however, continued to be downplayed by those wishing to exploit confidential data (such as health services and researchers) and even by data protection regulators. Nonetheless, GDPR allows data controllers to freely use anonymised data, though not without risk.[11] How to support patient confidentiality and still use patient data to support public health purposes remains a conundrum (see Health care).

Brazil's Marco Civil da Internet

Brazil's 2014 law, the Marco Civil da Internet, focused on ten pillars of digital human rights including network neutrality, digital privacy, freedom of expression, the right to cybersecurity, and universal access. The bill was considered a major victory for civil society. In order to speed the bill's passage, the government dropped a requirement for local storage of personal data that was inspired by Edward Snowden's 2013 revelations of endemic US spying.[12] Because the Cyberia cafe had supported the original cybercafe movement in Brazil,

[8] "Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality", by Marion Oswald, Jamie Grace, Sheena Urwin, and Geoffrey C. Barnes, *Information & Communications Technology Law*, 27:2, 223-250, DOI: 10.1080/13600834.2018.1458455: https://www.tandfonline.com/doi/pdf/10.1080/13600834.2018.1458455.

[9] "Simple Demographics Often Identify People Uniquely", by Latanya Sweeney, Carnegie Mellon University, Data Privacy Working Paper 3. Pittsburgh 2000: https://dataprivacylab.org/projects/identifiability/index.html,

[10] "Researchers: Anonymized data does little to protect user privacy", by Bryan Clark, The Next Web, 2019-07-30: https://thenextweb.com/insider/2019/07/30/anonymized-data-does-little-to-protect-privacy/.

[11] "Looking to comply with GDPR? Here's a primer on anonymization and pseudonymization", by Matt West, IAPP: https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/.

[12] "Brazil passes groundbreaking Internet governance bill", by Angelica Mari, ZDNet, 2014-03-26: https://www.zdnet.com/article/brazil-passes-groundbreaking-internet-governance-bill/.

Cybersalon had close contacts with the Brazilian internet governance community,[13] in developing the UK's version of the bill, it drew on many of the Marco Civil's pillars, in particular net neutrality. Dr Richard Barbrook (Cybersalon) contributed to making open source central to Brazilian digital architecture.[14]

Cambridge Analytica

The biggest data abuse scandal of the 2010s was undoubtedly Cambridge Analytica, which investigative journalist Carole Cadwalladr discovered had manipulated voters (see Democracy) in both the 2016 EU referendum and the 2016 US presidential election,[15] as well as previous campaigns in Trinidad and elsewhere. Cambridge Analytica began by collecting profiles of Facebook users by paying them to take a personality quiz that allowed the company to harvest their profiles and those of their friends. Matching the Facebook data to other consumer datasets that the company bought allowed the company to find emotional triggers allowing it to craft individual messages for specific voters. In testimony to the select committee for the Department for Digital, Culture, Media, and Sport, former Cambridge Analytica director Brittany Kaiser told MPs that she had been asked to devise a strategy to combine data collected by UKIP, Leave.EU, and Eldon Insurance, a company owned by Leave.EU backer Arron Banks in order to politically profile people and also said she had seen personally Eldon employees using insurance data to target people with political messages. In annual filings, Eldon says it holds data on 24.9 million British people; many are not customers, but had their detailed personal information forwarded when using price comparison services such as moneysupermarket.co.uk. Insurance companies also have access to police databases for fraud prevention.[16] In 2019, the ICO fined Leave.EU £15,000 for unlawfully using Eldon Insurance customers' details to send almost 300,000 political marketing messages, and £45,000 for sending an Eldon marketing campaign to political subscribers (a violation for which Eldon was fined £60,000).[17]

Cameras

The decade after the 9/11 attacks saw an acceleration in the spread of CCTV cameras throughout public and private places in the UK "for your safety". The

[13] "Brazil-London Cultural Highlights", by Nikki Gomez, Cybersalon, 2013-04-01: http://cybersalon.org/brazil-london-cultural-hotspots/.

[14] Cybersalon archives: https://lewissykes.info/archives/cybersalon/past.html.

[15] "The great British Brexit robbery: how our democracy was hijacked", by Carole Cadwalladr, *Observer*, 2017-05-07: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy.

[16] "Arron Banks, the insurers, and my strange data trail", by Carole Cadwalladr, *Guardian*, 2018-04-21: https://www.theguardian.com/technology/2018/apr/21/arron-banks-insurance-personal-data-leave-eu.

[17] "Leave.EU and Arron Banks insurance firm fined £120,000 for data breaches", by Alex Hern, *Guardian*, 2019-02-01: https://www.theguardian.com/uk-news/2019/feb/01/leave-eu-arron-banks-insurance-company-fined-data-breaches-information-commissioner-audit.

public generally supported the goals of safety, crime reduction, and capturing terrorists and murderers, and despite protests from privacy advocates the increasing number of cameras met with either apathy or popular approval. In the last decade the cameras have become networked, and the images, now stored for much longer, are increasingly identifiable via facial recognition; in 2019 police ran trials of automated real time facial recognition in public areas such as Oxford Circus despite reports that the systems were wildly inaccurate (see Facial Recognition). Meanwhile, the 2010-2011 explosion of smartphones (in 2010, Apple iPhone users rose from 8 million to 100 million), however, created a step change in visual surveillance: suddenly, everyone was carrying a camera that tagged every image with a time stamp and location and circulating the photos on social media, creating the "selfie" culture that then fuelled the rise of Instagram (founded 2010) and made Facebook the largest host of photographs in the world.

Centralisation

The original conceptions of both the Internet and the World Wide Web were highly decentralised, providing protection against censorship and detailed tracking. To a large extent, this was still the case in 2010. Between 2010 and 2020, however, the Internet became increasingly centralised, partly fuelled by the rise of smarphones and mobile apps, which tended to reinvent the Internet as a small selection of walled gardens. Google became dominant in search, in mobile operating systems through Android, and navigation, through its maps. Facebook became dominant in interconnecting people, and in countries where Facebook was excluded from data plans, it became synonymous with "the Internet".

By 2019, Google, Amazon, Facebook, Microsoft, Apple, and scores of brokers unknown to the general population had almost complete oversight of personal online footprints. From email, calendars, and team collaboration services to online healthcare, shopping, and banking, nearly all data somehow ends up with one of the big cloud providers, continually increasing the power gap between the individual user and the data-hosting tech giants. That trajectory developed exponentially. The more we use the Internet and carry and use smartphones, the more data we generate; as Internet of Things devices such as smart speakers become embedded in our homes every aspect of our daily lives will be captured and exploited by these invisible actors.

In a telling example of the change, Iranian blogger Hussain Derakshan emerged in 2018 from a ten-year jail sentence to discover that independent blogs had disappeared, social media had become indispensable, and his audience had shrunk from 20,000 reader to three Likes because in his missing decade social media algorithms had become the major factor in determining which stories get distributed and seen and diverted the revenue to the platforms.[18]

Children

Children had long been the canaries in the privacy coalmine for two reasons: first, because their online safety was the excuse for many moves toward

[18] "The Web We Have to Save", by Hossein Derakhshan. Medium, 2015-07-14: https://medium.com/matter/the-web-we-have-to-save-2eb1fe15a426.

censorship and control of the Internet; and second, because they themselves were the subjects of comprehensive state tracking through databases recording everything they did in school and then by using algorithmic systems to try to predict which might be at risk of abuse and, through the Prevent programme, which might be in danger of radicalisation and require intervention. By 2020, a few organisations such as DefendDigital.me and 5Rights had begun to campaign for children's rights including privacy and access to information. By then, it was also well understood that children may have smartphones (saturation was nearly 98% for under-17s) but not laptops or home broadband, so are unable to pursue their schooling from home in any meaningful way.

Competition

A major factor in the unparalleled size of companies like Google, Apple, Facebook, and Amazon is that in recent decades the US Federal Trade Commission, which is the agency in charge of enforcing competition law, has evaluated corporate behaviour and mergers solely by whether they raise or reduce prices. With so many technology companies offering "free" - in reality, pay-with-data, services, this approach has failed to stop numerous acquisitions that removed start-up competitors from the field. To some extent, the EU acted to protect competition where the US had stopped after 1998, when the Department of Justice sought to break up Microsoft into one unit for operating systems another for other software. The most notorious failure in the 2010s was Facebook, which promised EU investigators that in acquiring Instagram (2012) it and WhatsApp (2014) it would keep the services separate. Facebook's 2016 announcement that it would merge the three user databases led the EU to fine the company €110 million for providing incorrect or misleading information at the time of the sale. After taking over as European commissioner for competition in 2014, Margrethe Vestager pursued a number of other interventions against the big technology companies, including fining Google $5 billion in 2018 for illegal restrictions attached to Android. In 2019 she proposed to turn her attention to the competition risks of big data holdings.[19]

Content

Traditional media such as newspapers and broadcast television had little ability to track in detail what their readers and viewers chose to focus on. As web analytics became more sophisticated, this changed. Today, the owner of a content website can tell in detail which pages are most popular and which pages are widely shared and draw traffic. Cable television began to change this, as set-top boxes collected data on what their owners watched and for how long; personal video recorders such as the Tivo also created large amounts of viewing data for their suppliers. The rising popularity of streaming services such as Netflix, the BBC's iPlayer, and Amazon Prime video, plus the arrival of "smart" televisions with Internet connections, however, mean that few viewers can now avoid having

[19] "Europe's antitrust chief, Margrethe Vestager, set for expanded role in next Commission", by Natasha Lomas, TechCrunch, 2019-09-10: https://techcrunch.com/2019/09/10/europes-antitrust-chief-margrethe-vestager-set-for-expanded-role-in-next-commission/.

their choices directly monitored by third parties. This is also true of some types of ebooks and readers; for example, through the Kindle Amazon can tell what pages and paragraphs users read, and has proposed to change how it pays authors royalties from a fee per book to a much finer-grained system that rewards them only for the exact percentage of the book that gets read.[20]

Connected cars

In the 2010s cars rapidly became data collectors and were adding Internet access, allowing mechanics to perform remote diagnostics and granting drivers and passengers access to real-time traffic conditions, updated maps, and entertainment.

Even within these limits - connected cars carry embedded mobile broadband chips, 40-plus microprocessors, and dozens of sensors, but not the vast array of computing power and sensors autonomous cars require - in 2015 Hitachi estimated that connected cars would upload 25GB of data to the cloud per hour, including the car's route, speed, components' life cycles, and road conditions, driver behaviour, and other telematics that local and central governments hope to use to improve roadway design.[21] The change led to new security risks that car manufacturers never had to consider before,[22] including the theft of personal data, remote manipulation of safety-critical systems, and theft of personal data. Security researchers began sounding the alarm in 2013.[23] In another unconsidered risk, Teslas retain all the data that drivers voluntarily store plus all the information the cars generate and collect and are not wiped in the cars it resells or the crashed models found in junkyards.[24]

On the plus side, increased connectivity has improved the driving experience. Tesla's over-the-air patching adds features and real-time trend analytics enable preventive maintenance, while geolocation helps track stolen or misplaced cars, and many drivers like the car's assistance in parking.

Autonomous cars - if they become reality - will be even bigger data hogs. In 2018, Intel predicted they would consume and generate about 40TB of data per eight hours of driving. One million such cars would generate as much data as

[20] "You don't get paid unless people actually read your book: the new Kindle Unlimited royalties", by Kirsten Reach, Melville House, 2020-06-16: https://www.mhpbooks.com/you-dont-get-paid-unless-people-actually-read-your-book-the-new-kindle-unlimited-royalties/.

[21] "Connected cars will send 25 gigabytes of data to the cloud every hour", by kdespagniqz, Quartz, 2015-02-13: https://qz.com/344466/connected-cars-will-send-25-gigabytes-of-data-to-the-cloud-every-hour/.

[22] "Top 10 Security Challenges in the Automotive Industry for Connected Cars", by Tim Hodkinson, Trustonic, 2019-09-16: https://www.trustonic.com/news/blog/top-10-security-challenges-for-connected-cars/.

[23] "Cracking the Computer on Wheels", by Wendy M. Grossman, Infosecurity, 2013-08-20: https://www.infosecurity-magazine.com/magazine-features/cracking-the-computer-on-wheels/.

[24] "Tesla cars keep more data than you think, including this video fo a crash that totaled a Model 3", by Kate Fazzini and Lora Koloday, CNBC, 2019-03-29: https://www.cnbc.com/2019/03/29/tesla-model-3-keeps-data-like-crash-videos-location-phone-contacts.html.

nearly 3 billion people.[25] As of 2019, the UK has an estimated 38 million cars on the road.

Cookies

Cookies began as a harmless way of giving web pages memory to enable persistent shopping baskets. However, they were quickly hijacked by the advertising industry and put to work tracking people browsing online, and, ignoring objections from activists and the Internet Engineering Task Force, Netscape and Microsoft, the two leading browsers, both enabled third-party cookies, kicking off the Internet data grab in earnest. Many advertisers had been looking for alternative solutions on the assumption that the IETF would prevail; in 2000, however, IETF revised its recommendations to formally accept third-party cookies.[26]

By 2001, the EU was considering regulation; the 2009 ePrivacy Directive, which came into effect in 2011, required opt-in consent before cookies could be placed on user machines, and set off a wave of notices that popped up on almost every website. GDPR's requirement for explicit consent set off a second wave of more complex controls and caused some (chiefly American) news sites to block EU visitors entirely. In 2020, Google announced it would phase out cookies in its Chrome browser by 2022.[27] Critics saw the move as a way of increasing the company's dominance over advertising.

Cryptocurrencies

In 2008, when the arrival of bitcoin launched a wave of cryptocurrencies, it was commonly believed that such payments were untraceable. This mythology began to fade in 2013, when police were connected a user name that promoted the dark market Silk Road site on multiple sites to a posting looking to hire a bitcoin expert; the combination let them trace more than 700,000 bitcoin transactions from seized Silk Road servers to Ross Ulbricht's personal laptop.[28] In 2016 security researchers showed that individual users can be traced by surveilling the entire network, and large transactions can be traced even when cloaked by mixing services. Once an address is identified all associated transactions are revealed.[29]

[25] "Think Your Cellphone Uses a lot of Data? Report Claims Autonomous Cars Will Use 4,000 GB in one Day", by Vineeth Joel Patel, Future Car, 2020-04-18: https://www.futurecar.com/876/Think-Your-Cellphone-Uses-a-lot-of-Data-Report-Claims-Autonomous-Cars-Will-Use-4000-GB-in-one-Day-.

[26] "RTF 2965: HTTP State Management Mechanism" by IETF, October 2000: https://tools.ietf.org/html/rfc2965.

[27] "Google Chrome Will Phase Out Third-Party Cookies by 2022", by Ronan Shields, *Adweek*, 2020-01-14: https://www.adweek.com/programmatic/google-chrome-will-phase-out-third-party-cookies-by-2022/.

[28] "Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop", by Andy Greenberg, *Wired*, 2015-01-29: https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/.

[29] "Why criminals can't hide behind Bitcoin", by John Bohannon, *Science*, 2016-03-09: https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin#.

Data breaches

Among myriad massive data breaches, the three most influential in the UK were the extramarital dating site Ashley Madison (2015), UK ISP TalkTalk (2015), and the credit reporting agency Equifax (2017). Ashley Madison was the target of the Impact Team hacking group, which stole users' personal information including home addresses, search histories, and credit card numbers. The website's salacious nature meant wide coverage, and some users received emails demanding bitcoin payments to keep the hackers from sharing the information with the user's spouse. The resulting stress on the families involved - in a few cases, leading to suicide - led the press to argue that the site should be taken down and cease trading. In the TalkTalk breach, attackers took advantage of poor security practices to use SQL injection to access the personal data of 150,000 subscribers, including sensitive financial data for more than 15,000 of them. The Information Commissioner's Office eventually fined the company £400,000 for its "failure to implement the most basic cyber security measures".[30] At the time the Equifax data breach, which the company did not detect for at least six weeks, was one of the largest ever; among the compromised data of 143 million Americans were social security numbers, birth dates, addresses, driver's licence numbers, credit card numbers, and even passport data in some cases. The compromised data of 400,000 Britons was less sensitive: dates of birth, email addresses, and telephone numbers. Equifax eventually paid over $700 million to settle complaints from the US Consumer Financial Protection Bureau, the Federal Trade Commission, and 48 states, the District of Columbia, and Puerto Rico. The ICO fined the company £500,000, the maximum available at the time.[31] Unlike Ashley Madison or TalkTalk, consumers have no choice about being included in Equifax's databases: credit scores are an essential part of being able to function in modern life, leading the social scientist Zeynep Tufecki to observe that we were not Equifax's users but its victims.

Democracy

Since at least 2010, Jeff Chester at the Center for Digital Democracy had been warning that the same profiling that was benefiting advertisers could be repurposed to target and manipulate individual voters to benefit specific political actors.[32] The Cambridge Analytica scandal (see Cambridge Analytica) showed that this future had arrived. In the US, the 2018 Mueller report showed that Russian interference via a sophisticated operation had sowed discord among

[30] "TalkTalk hit with record £400k fine over cyber-attack", by Alex Hern, *Guardian*, 2016-10-05: https://www.theguardian.com/business/2016/oct/05/talktalk-hit-with-record-400k-fine-over-cyber-attack.

[31] "Credit reference agency Equifax fined for security breach", Information Commissioner's Office, 2018-09-20: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/credit-reference-agency-equifax-fined-for-security-breach.

[32] "The grey hour", by Wendy M. Grossman, *net.wars*, 2011-07-09: http://www.pelicancrossing.net/netwars/2011/07/the_grey_hour.html.

social media users in 2016;[33] further investigation by academic researchers suggested that the result helped Donald Trump attain the presidency.[34]

Few understand the extent to which they can be manipulated via online advertising. In 2018, Facebook finally released the ads run by the official Vote Leave campaign in 2016. Of the 1,433 different messages that were released, many focused on ending immigration; others tied the EU to abusing animals, regulating Uber, failing to protect polar bears, limiting Britain's flood defences, and restricting innovation. Collectively, they were viewed millions of times.[35]

Digital bill of rights

There had been similar proposals before, particularly in 2012, when then-US president Barack Obama proposed a set of privacy rights for Americans, but after the shock of Edward Snowden's revelations of government surveillance in 2013, a movement began to build for a Digital Bill of Rights for Internet users in Brazil, Italy, and Britain, where the push was led by Cybersalon.[36] Cybersalon, which had close contacts with the Brazilian Internet community, drew on the pillars of the Marco Civil, particularly net neutrality, to develop a UK version. In November 2014. Cybersalon's open letter, "From Digital Pioneers to Digital Natives", asked MPs and industry leaders to adopt the pledges; the document also served as a key discussion point at a cross-party 2014 House of Commons meeting that identified key demands and proposed a framework. Labour's interest derived from the history of surveillance aimed at union activists; fearing that digital social media platforms would become a vector for surveillance, the TUC organised workshops on the risks of digital media and held consultations with the unions. All of this, plus several public consultations, fed into the eight demands that made up the 2016 version of the Digital Bill of Rights,[37] which became the subject of a second Cybersalon-led House of Commons meeting[38] and a consultation with Italian activists, who later proposed a Digital Bill of Rights for their own country. This version became the core framework for the Labour Party's

[33] "Mueller indictment reveals sophisticated Russian manipulation effort", by Harper Neidig, The Hill, 2018-02-16: https://thehill.com/policy/technology/374306-mueller-indictment-reveals-sophisticated-russian-manipulation-effort.

[34] "How Russia Helped Swing the Election for Trump", by Jane Mayer, *The New Yorker*, 2018-09-24: https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump.

[35] "Vote Leave's targeted Brexit ads released by Facebook", BBC, 2018-07-26: https://www.bbc.co.uk/news/uk-politics-44966969.

[36] "Digital Bill UK: The Story So Far", by Cybersalon: http://cybersalon.org/digital-bill-uk-the-story-so-far/.

[37] "Digital Bill of Rights UK", by Cybersalon, 2016: http://cybersalon.org/digital-bill-of-rights-uk/.

[38] "Wendy Grossman introduces Cybersalon Net Bill of Rights debate": https://www.youtube.com/watch?v=ygOJS5wS9b4.

2016 Digital Democracy Manifesto.[39] The key points from Cybersalon's Digital Bill of Rights were universal access and the open-source release of all publicly funded software and hardware. These elements were carried forward to the 2019 Labour manifesto with an increased focus on universal access, given the increasingly uneven geographical coverage of broadband in the UK and the lack of quality Internet access that barred children in many inner-city homes from doing homework online. After a third period of consultation a new version of the bill began development in 2020 with the politics department at Westminster University and the media studies department at Middlesex University that incorporated new work on children's digital rights with respect to gaming and online services.

Digital payments

In 2008, 60 percent of all British payments were conducted in cash. By 2018, cash payments had dropped to 28 percent; by 2019 10 percent of adults were living a largely cashless life, rising to 17 percent among those aged 25 to 34.[40] In between, both smartphones and credit cards began incorporating near-field communication, first launched in a payment card by Barclaycard in 2007, followed by Apple Pay (released 2014), Google Pay (2015), Square (2009), Stripe (2010), iZettle (2010), and many others. While NFC added convenience to many transactions - the banks set the system up so that PINs were not needed for amounts under £30 - the increasing use of digital payments in preference to anonymous cash meant that a far higher percentage of the UK's payments were being recorded and tracked, a trend enhanced by the move to online purchasing. A sense of how valuable transaction data can be can be seen by a 2018 in which Mastercard received millions of dollars in return for providing Google with "anonymised" customer data (see Anonymisation), which Google uses to link offline purchases to online identities and Maps data in order to show whether people who click on online ads go on to complete purchases at retail stores.[41] On transport systems, digital payments also changed systems such as the London Underground from being a predominantly anonymous service to one where most passengers can be tracked individually through the system.

Drones

As of 2019, the biggest publicity surrounding drones in the UK was an incident in which Gatwick Airport shut down for most of a day after a few drones were sighted near a runway. However, as they become more available and are

[39] "Full text: Jeremy Corbyn's speech at digital democracy manifesto launch", by Jeremy Corbyn, Labour List, 2016-08-16: https://labourlist.org/2016/08/full-text-jeremy-corbyns-speech-at-digital-democracy-manifesto-launch/.

[40] "One in 10 adults in UK have gone 'cashless', data shows", by Rupert Jones, *Guardian*, 2019-06-06: https://www.theguardian.com/money/2019/jun/06/adults-uk-cashless-contactless-payments.

[41] "Google reportedly bought Mastercard data to link online ads with offline purchases," by Shannon Liao, The Verge, 2018-08-30: https://www.theverge.com/2018/8/30/17801880/google-mastercard-data-online-ads-offline-purchase-history-privacy.

increasingly equipped with high-quality cameras (and, soon, microphones), the potential for privacy invasion is becoming a known issue. Under the regulations in force in 2019, drones must avoid designated "no-fly" zones, which include airports and prisons, and consumer drones (those under 20kg in weight) may not be flown higher than 400 feet and must be kept at least 50 metres away from people and private property and 150 metres away from congested areas and organised open-air gatherings of more than 1,000 people. Larger drones require registration, and the police are pushing for geofencing technology that would be built into drones and automatically keep them out of no-fly areas.[42]

Encryption

The importance of using encryption to protect data in transit (communications) and at rest (stored data) is one area where the tech giants have typically held the line to protect privacy interests of their customers against the state. After a 2015 shooting attack in San Bernardino, California, the FBI asked Apple to write software to break into the shooters' phones in order to determine whether they had collaborators. Apple CEO Tim Cook refused. The case was dropped in court after the FBI contracted a third-party company to break into the encrypted phones. Privacy campaigners supported Apple's stand, arguing that compelling Apple to break the phones' encryption would pit privacy versus national security and the implications would be far-reaching as the software would be a target for hackers and criminals seeking ways to break into people's phones for their own purposes. Shortly afterwards, Facebook opted to turn on end-to-end encryption for messages sent via its WhatsApp subsidiary, at a stroke giving strong encryption to 1 billion users worldwide.[43]

Facial recognition

Image recognition and language translation were among the first uses for the improved machine learning (see AI) of the 2010s because of the large-scale availability of publicly posted material on the web that could be repurposed as training data. In 2019, the world learned that researchers at universities and companies like IBM had appropriated images collected by companies like Facebook (founded 2004), Flickr (2004), and Instagram, as well as video images of students traversing college campuses, and used them to train data machine learning systems that were then supplied to police forces and agencies such as US Immigration and Customs Enforcement.[44] Individuals who had innocently posted photos share with friends were horrified. In 2018, Big Brother Watch called

[42] "UK Drone Laws Explained: Where can and can't I fly my drone in 2019", by Aatif Sulleyman, Trusted Reviews, 2019-07-05: https://www.trustedreviews.com/news/uk-drone-laws-2019-3146402.

[43] "Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People", by Cade Metz, *Wired*, 2016-04-05: https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/

[44] "Facial recognition's 'dirty little secret': Millions of online photos scraped without consent", by Olivia Solon, NBC News, 201-03-12: https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.

attention to police trials of real-time automated facial recognition, initiated without public debate. Even though 98% of the systems' "matches" wrongly identified innocent people,[45] trials continued, both private, as in Kings Cross area in 2019, where the developer concerned notified neither public nor government,[46] and public, such as the Stratford Centre shopping mall[47] and outside Oxford Circus tube station in 2020.[48] By then, claims were appearing that facial recognition could also accurately estimate the subject's age, and its adoption by retailers and others, who share the results with peers to effectively blacklist people previously accused of shoplifting or stalking.[49]

General Data Protection Regulation

The EU had long planned to update the 1995 Data Protection Directive, which was formulated during an era when the Internet was still decentralized; Google and the social media companies didn't exist; Apple was a niche company; and Amazon was in its first year of operation. Among the changes being discussed in the early 2010s were the "right to be forgotten"; greater enforcement powers for regulators; and strengthened citizens' rights. The big technology companies mounted the biggest lobbying operation in EU history to oppose this expansion, and political will might have faded but for Edward Snowden's 2013 revelations that the "Five Eyes" were collaborating on spying on everyone else via secret deals and tools. With revived interest, GDPR was passed in 2016, shepherded through the European Parliament by the German MEP Jan-Philipp Albrecht and came into force in 2018.[50] By then, the growing Internet of Things and the arrival of physical-world tracking meant that it was already out of date. Some of the rights incorporated into GDPR had been proposed for the Digital Bill of Rights in both Italy and the UK (see Digital Bill of Rights).

Gambling

Gamblers have the highest lifetime value to advertisers; as a result, the explosion of gambling enabled by mobile phones in the 2010s - revenues rose

[45] "Face Off: The lawless growth of facial recognition in UK policing", by Silkie Carlo, Jennifer Krueckeberg, and Griff Ferris, Big Brother Watch, 2018-05-05: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf.

[46] "King's Cross developer defends use of facial recognition", by Zoe Kleinman, BBC, 2019-08-12: https://www.bbc.co.uk/news/technology-49320520L.

[47] "Met police deploy live facial recognition technology", by Damien Gayle, *Guardian*, 2020-02-11: https://www.theguardian.com/uk-news/2020/feb/11/met-police-deploy-live-facial-recognition-technology.

[48] "Police use live facial recognition technology at Oxrford Circus", by ITV News, 2020-02-20: https://www.itv.com/news/london/2020-02-20/police-use-live-facial-recognition-technology-at-oxford-circus/.

[49] "With facial recognition, shoplifting may get you banned in places you've never been", by Alfred Ng, CNet, 2019-03-20: https://www.cnet.com/news/with-facial-recognition-shoplifting-may-get-you-banned-in-places-youve-never-been/.

[50] *Democracy - Im Rausch der Daten*, directed by David Bernet, 2015: https://www.bpb.de/mediathek/254194/democracy-im-rausch-der-daten.

from £8.4 billion in 2011 to £14.4 billion in 2018[51] - was an extra kick to making personal data valuable. Driven by the ease of use and innovation of smartphone-based betting platforms, the proportion of people gambling weekly rose to 32%. The ease of access via computer games ("skins betting") and social media meant that by 2017 about 25,000 11-to-16-year-olds had become problem gamblers, and more than 10% of children reported having played casino-style games.[52]

Gig economy

The rise of the web and then smartphones created new opportunities, first for sharing company-owned resources (Zipcar), then for exploiting underused personal resources such as cars (Uber) and spare rooms (Airbnb), and finally for ad hoc employment as the widespread availability of geolocation made it vastly more efficient to match drivers to nearby passengers, hungry people to food, or workers to tasks for completion. In all cases, the companies painted a rosy picture of the flexibility and opportunities of the "sharing economy".[53] The "sharing" proved to be one-way; Platform workers, who include task workers on Amazon's Mechanical Turk and in near-invisible jobs inside all these operations, do not see the operational data their companies collect or the algorithms that determine who gets work. The result greatly increased the imbalance of power at the expense of workers' rights while turning work into a relentless series of tasks.[54] By the late 2010s workers were beginning to fight back by petitioning national courts for employment rights. In a 2017 UK Deliveroo strike that won drivers employment rights, technology proved to be both the problem (Deliveroo's platform design) and the solution (strike leaders used social media to create a pop-up union).[55]

Health care

National public health systems are a particular temptation for data-driven start-ups. In the UK, finding the balance between the public good and patient confidentiality has been a long-running saga.[56] In 2014, the NHS had to withdraw the "care.data" programme after the public objected to its proposal to sell the nation's health data to commercial researchers. In 2016, the AI company DeepMind, which Google acquired in 2014, signed a deal with the Royal Free NHS trust that granted it access to a wide range of health care data pertaining to

[51] "Gambling industry in the United Kingdom (UK) - Statistics & Facts", by David Lange, Statista, 2020-03-23: https://www.statista.com/topics/3400/gambling-industry-in-the-united-kingdom-uk.

[52] "25,000 children in Britain are problem gamblers, report finds", by Rob Davies, *Guardian*, 2017-12-17: https://www.theguardian.com/society/2017/dec/12/children-britain-problem-gamblers-report.

[53] *What's Yours Is Mine: Against the Sharing Economy*, by Tom Slee, OR Books, 2015.

[54] *Ghost Work*, by Mary L. Gray and Siddharth Suri, Houghton Mifflin, 2019.

[55] "Boss or spy - how data killed office trust", Cybersalon, 2018-01-13: http://cybersalon.org/boss-or-spy-how-data-killed-office-trust/.

[56] "Latest health privacy scandal", by Ross Anderson, Light Blue Touchpaper, 2014-04-04: https://www.lightbluetouchpaper.org/2014/04/04/.

the 1.6 million patients that pass each year through the three hospitals the trust runs without asking their permission. medConfidential objected to Google's being awarded control over the UK's health data analytics.[57] In 2018, even though Google had promised in 2014 that the data DeepMind acquired as the result of its deals with the Royal Free would not be merged with other personal data it held, it subsumed DeepMind into the new US-based initiative, Google Health.[58] The Information Commissioner's Office ruled that the deal with Royal Free Hospital was illegal and that Royal Free failed to comply with the UK's Data Protection Act (1998). However, the ICO did not stop the the real-time transfer of patient data.[59]

Internet of Things

The mid-2010s saw the early stages of the arrival of the Internet of Things, bringing internet-connected TVs, smart speakers, and other devices into people's homes. The arrival into the market of manufacturers with no experience in computer security coupled with low margins and pressures to keep costs down brought security vulnerabilities and data breaches into individual homes. Over the longer term, the data collected by these devices will give advertisers and others unprecedented access to our intimate personal lives. By 2020, smart speakers had reached the homes of 22% of the British population, up from 9% in 2017.[60]

Italian Digital Bill of Rights

The 2015 Cybersalon presentation of a UK Digital Bill of Rights was swiftly copied: a committee of the Italian parliament published the Declaration of Internet Rights, which built on its UK and Brazilian counterparts. It focused on two things: Internet access as a fundamental right and network neutrality, which was increasingly under pressure from commercial companies. Following an open consultation and an online debate with 600 contributions, the Italian bill, which was intended to become a contribution to international debates rather than a piece of legislation added "rights to online knowledge and education"; interoperability, data portability, and open source software. These were all seen as curbs to the power of the American technology companies, an aspect that became increasingly important. The Italians were first to recognise that the core components of digital privacy included the "right to be forgotten" (over Google's objections) and the

[57] "Revealed: Google AI has access to huge haul of NHS patient data", by Hal Hodson, *New Scientist*, 2016-04-29: https://www.newscientist.com/article/2086454-revealed-google-ai-has-access-to-huge-haul-of-nhs-patient-data/.

[58] "Google swallows up DeepMind Health and abolishes 'indepenent board'", by Andrew Orlowski, The Register, 2018-11-14: https://www.theregister.co.uk/2018/11/14/google_swallows_up_deepmind_health_and_abolishes_independent_board/.

[59] "Royal Free breached UK data law in 1.6m patient deal with Google's DeepMind", by Alex Hern, *Guardian*, 2017-07-03: https://www.theguardian.com/technology/2017/jul/03/google-deepmind-16m-patient-royal-free-deal-data-protection-act.

[60] "Smart speakers reaching 'mass adoption' in UK (but concerns around privacy grow), by Robin, NetImperative, 2020-01-06: http://www.netimperative.com/2020/01/06/smart-speakers-reaching-mass-adoption-in-uk-but-concerns-around-privacy-grow/.

right to anonymity. Many of these rights were eventually incorporated into the EU's GDPR (see General Data Protection Regulation).[61]

Investigatory powers

The 1990s saw an extended public debate on law enforcement access to encrypted communications, which culminated in the passage of the Regulation of Investigatory Powers Act (2001) to regulate interception. The 9/11 attacks led to the enshrinement of communications data retention under the Anti-terrorism, Crime, and Security Act (2003). Edward Snowden's 2013 revelations of government spying led to the hasty passage of the Data Retention and Investigatory Powers Act (2014), which contained a sunset clause to ensure a more thought-out replacement in 2016.[62] Nonetheless, the speed and lack of scrutiny of DRIPA's passage led the MPs Tom Watson (Labour-West Bromwich East) and David Davies (Con-Haltemprice and Howden) to bring a case against the government in the European Court of Justice. In 2016, the ECJ ruled DRIPA unlawful. By then, however, it was being replaced with the Investigatory Powers Act, which could be seen as legalizing all the illegitimate spying Snowden warned was taking place; it contains, among others, provisions allowing device "interference", bulk collection of communications data, retention of Internet connection records for one year with access allowed as part of a targeted investigation without a warrant, and a requirement for UK, though not foreign, communications service providers to be able to remove encryption that they apply.

Lock-in

"Lock-in" is a state prized by businesses; it means that for one reason or another - contract terms, functionality, or legacy systems - customers are not free to change to a competitor. Although it seems like it ought to be simple to shift from one search engine to another, or one word processor to another, whether online or locally hosted, in practice users become accustomed - trained - to the systems they're used to. Economists talk of "switching costs" in purely financial terms, but for many users the cognitive burden of learning a new system or the logistical burden of unpicking multiple systems embedded in how they manage their work and lives and trying to convince their friends and family to switch are even bigger deterrents. Once a person's working life is locked into Gmail/Google Docs/Google Calendar or Apple apps and iCloud via their phone, they are effectively forced to "consent" to to data exploitation even though under the 2018 General Data Protection Regulation consent is required to be meaningful. These lock-in factors have contributed to the winner-takes-all dominance of Google, Facebook, Amazon, and Apple.

[61] "Italy Issues a Declaration of Internet Rights - Now Let's Improve It", by Elisabetta Ferrari, CGCS Media Wire, 2015-08-04: http://global.asc.upenn.edu/italy-issues-a-declaration-of-internet-rights-now-lets-improve-it/.

[62] "'Emergency' Ushers in a New Era in British Communications Surveillance", by Wendy M. Grossman, *IEEE Security & Privacy*, , 12(6), 84–88. doi:10.1109/msp.2014.106: https://www.computer.org/csdl/magazine/sp/2014/06/msp2014060084/13rRUyeCk8q.

Moderation

Keeping online services free of unwanted material such as child abuse images, violence, abuse, extremism, and misinformation is an issue that goes back to the earliest days of the internet. In the US, Section 230 of the 1996 Communications Decency Act has held platforms free of liability for material users posted. Over time, as pressure mounted from all sides - governments, advertisers, and users - platforms like Facebook and YouTube began hiring thousands of raters to make content decisions too nuanced for algorithms. Sited everywhere from the US to the Philippines, those outsourced agency workers are are hidden, low-paid, low-status part of the Internet economy who must make high-speed decisions about many hours of upsetting material following rules that have developed over time on a case-by-case basis[63] or, in the case of Google's search engine, ensuring that ads don't run alongside offensive content.[64] During the coronavirus crisis, the time it took to accept an image for Facebook advertising grew from 12 hours to 36 hours, as moderators got swamped by an avalanche of virus-released misinformation. However, the picture is complicated by the fact that all social media relies on outrage as a driver of user engagement.[65] The Open Rights Group has opposed privatising censorship by putting the platforms in charge.[66]

Open data

As the Guardian's technology editor from 2005 to 2014, Charles Arthur masterminded a campaign to open up public data. In 2012, the government began opening up public datasets and put £10 million in funding into setting up the Open Data Institute, founded by Nigel Shadbolt and web inventor Tim Berners-Lee, to be a world leader in inspiring people and businesses to innovate with data. Alongside this initiative, the Cabinet Office also set up the Government Digital Service (2011) and staffed it with established technology innovators. GDS was intended to revamp government use of IT to emulate the convenience and usability people were accustomed to from commercial services, as well as reform government IT procurement to include smaller, local companies and avoid the huge, failed IT projects of the past

Politics

The Cambridge Analytica scandal, in which political operatives exploited data extracted from Facebook in order to build profiles and tightly target their messaging, is widely believed to have played a large part in Britain's vote to leave

[63] *Behind the Screen: Content Moderation in the Shadows of Social Media*, by Sarah T. Roberts, Yale University Press, 2019.

[64] "The secret lives of Google raters", by Annalee Newitz, Ars Technica, 2017-04-27: https://arstechnica.com/features/2017/04/the-secret-lives-of-google-raters/.

[65] "A Better Internet Is Waiting for Us", by Annalee Newitz, *New York Times*, 2019-11-30: https://www.nytimes.com/interactive/2019/11/30/opinion/social-media-future.html.

[66] "UK and France propos automated censorship of online content", by Ed Johnson-Williams, Open Rights Group, 2017-06-13: https://www.openrightsgroup.org/blog/2017/uk-and-france-propose-automated-censorship-of-online-content.

the EU and the election of US president Donald Trump, both in 2016. However, exploiting data played an important role in both of Barack Obama's election victories, and in the UK has become embedded in the activities of all three main political parties. During the 2019 election, the Open Rights Group developed a web tool to make it easy for individuals to issue GDPR subject access requests for their personal data from the political parties; the results of numerous such requests showed that although the parties enjoy legal exemptions to data protection law that allow them to process sensitive data a lack of enforcement means the parties are using political profiling techniques that may be illegal as well as unethical.[67]

Privacy policies

As data protection law has expanded, privacy policies stating how a site or service will handle user data have become more complex. Ideally, nothing more should be required than a reminder that the site complies with applicable laws. However, most companies view privacy policies, like their terms of service, as exercises to protect themselves from liability, and as a result are vastly longer and claim far more rights than necessary. Researchers who have studied these policies say that consumers universally loathe reading them; that creating standards for what should and should not be included would help; and even better would be designing privacy in from the beginning - the opposite of what many of today's companies want to do.[68]

Terms of service

"The biggest lie" on the internet is the click users make to indicate they have read the terms of service before creating an account on a new system. Like privacy policies, terms of service are essentially corporate lawyer efforts to shield the company from liability; unlike privacy policies, terms of service lay out how users may and may not use the service. Typical terms of service include provisions barring abuse of other users and the system itself, copyright claims for both the material the service provides and material the user uploads, and conditions for dispute resolution, often requiring users to accept arbitration in foreign jurisdictions. These agreements expanded even more when smartphones became mass market items. In 2016 the Norwegian Consumer Council proved the point by staging a live reading of the terms and conditions for an Apple iPhone plus the 33 apps an average Norwegian had their phone. The documents added up to 250,000 words, and took 30 hours to read aloud.[69]

Travel

[67] "Exposing abuse of personal data in political campaigning", by Open Rights Group: https://www.openrightsgroup.org/campaigns/who-do-they-think-we-are-exposing-abuse-of-personal-data-in-political-campaigning.

[68] "Do you agree not to read our privacy policy?", by Wendy M. Grossman, *Guardian*, 2008-01-10: http://www.guardian.co.uk/technology/2008/jan/10/privacy.it.

[69] "250,000 words of app terms and conditions", by Øyvind H. Kaldestad, Norwegian Consumer Council (Forbrukerrådet), 2015-05-24: https://www.forbrukerradet.no/side/250000-words-of-app-terms-and-conditions/.

The 9/11 attacks led to a massive increase in airport security; it became impossible to fly without identity documents, and both the US and the EU developed policies requiring travellers to provide increased background information for them to analyse in advance of flights. By 2020, most airline travel in the US and EU required 24 hours' notice for checking against no-fly lists. On the local level within the UK, the period between 2003 and 2020 saw travel on the London Underground and other local systems change from being predominantly anonymous (cash paid for paper tickets) to predominantly identified (card payments and identity-linked smart cards). This was exacerbated as Transport for London began to move away from single-purpose Oyster cards toward NFC payments directly from credit cards or mobile phones (see Digital Payments).

Universal access

A frequently-heard complaint that surfaced in Cybersalon's public consultation at the 2015 Web We Want festival was lack of reliable broadband access. In a 2016 test, the British villages with the slowest broadband were reporting that speeds were such that it would take five days to download a high-definition movie.[70] As a result, Cybersalon considered universal broadband the most important of the elements included in the Digital Bill of Rights. Recognising the potential economy-changing implications, Labour included nationalising BT's broadband arm and free broadband for all in its 2019 election manifesto.[71] The unevenness of broadband access across the UK would become an issue during the 2020 pandemic.

Workplace surveillance

The TUC's efforts to oppose workplace surveillance expanded after June 2016, when the union GMB found that ASOS and Sports Direct were using CCTV to monitor their warehouse workers. XPO Logistics and other similar organisations also acknowledged trialling CCTV cameras.[72] By 2020, it was well known that companies such as Amazon that operate large fulfillment warehouses were closely monitoring every move,[73] and many companies had begun installing software to monitor employees closely, cutting out the small but significant and needed moments of downtime such as the minute to breathe between phone calls or the time spent in the bathroom, an unexpected twist on the idea that robots

[70] "Britain's slowest broadband speeds: The village where it takes five days to download a film", *Daily Telegraph*, 2016-03-03: https://www.telegraph.co.uk/news/newstopics/howaboutthat/12182023/UK-slowest-broadband-speeds-revealed.html.

[71] "Labour's free broadband plan fires up the election battle", by Peter Walker, Rajeev Syal, and Heather Stewart, *Guardian*, 2019-11-15: https://www.theguardian.com/technology/2019/nov/15/free-broadband-essential-uk-compete-john-mcdonnell-labour-policy-openreach.

[72] "ASOS warehouse workers face constant CCTV monitoring and threat of random searches", by Hazel Sheffield, *The Independent*, 2016-06-08: https:/www.independent.co.uk/news/business/news/asos-sports-direct-zero-hours-cctv-security-monitoring-random-searches-a7070286.html

[73] "How Amazon automatically tracks and fires warehouse workers for 'productivity', by Colin Lecher, The Verge, 2019-04-25: https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

would take all our jobs.[74] Among academic researchers, Phoebe Moore explored the trend toward increasing worker surveillance and the "quantified worker",[75] and, in the US, Karen Levy has studied truckers and the arrival of in-cab monitoring, which is supposed to be for their safety but also grants the trucking companies greatly increased ability to monitor them, even when they are sleeping in their cabs.[76]

2020: After the virus

The SARS-CoV-2 pandemic abruptly created a global need, generally accepted as legitimate, to identify infected individuals and trace their contacts, enforce quarantine and lockdowns, and operate health checks in public places. As the virus spread to almost every country, emergency legislation enacting these measures followed.[77] In Britain, the Health protection (Coronavirus) Regulations 2020 and the Coronavirus Act 2020 allowed the government discretionary emergency powers to order shops, restaurants, theatres, pubs, and other businesses to close; detain people suspected of COVID-19 infection; suspend the operation of ports and airports; draft medical students and retired health care workers into the health services; among others. The Act also postponed the scheduled May 2020 local elections for a year. The act has a two-year time limit and must be reviewed every six months.

The uneven distribution of infections, hospitalisations, and deaths reflected society's general inequality. Infections clustered among people who lived or worked in crowded or communal situations - low-income people, immigrants, refugees, prisoners and their guards, and care home residents and workers. Deaths occurred disproportionately among those of black, Asian, minority, and ethnic backgrounds. A paper from the US National Bureau of Economic Research found that the digital divide was also a crucial factor: while differences in the ability to stay safely at home also correlated with income, the unequal availability of high-speed broadband was the biggest such driver and explained much of the inequality in the ability to self-isolate.[78] High-speed broadband was also crucial for children and others whose education had abruptly moved online and for whom the ability to participate equally was essential.

[74] "How Hard Will the Robots Make Us Work?"by Josh Dzieza, The Verge, 2020-02-27: https://www.theverge.com/2020/2/27/21155254/automation-robots-unemployment-jobs-vs-human-google-amazon.

[75] "The Quantified Self in Precarity: Work, Technology, and What Counts", by Phoebe V. Moore, Advances in Sociology series (Abingdon, Oxon: Routledge, Advances in Sociology series), 2018: ISBN 9781138674066.

[76] "Wearable Tech That Tells Drowsy Truckers It's Time to Pull Over", by Julie Weed, *New York Times*, 2020-02-06: https://www.nytimes.com/2020/02/06/business/drowsy-driving-truckers.html.

[77] "Tracking the Global Response to COVID-19, Privacy International, ongoing: https://privacyinternational.org/examples/tracking-global-response-covid-19.

[78] "Social Distancing, Internet Access, and Inequality", by Lesley Chiou and Catherine Tucker, National Bureau of Economic Research, 2020-04: https://www.nber.org/papers/w26982.pdf.

Common themes emerged around the world. Contact tracing has been a vital tool for epidemiologists since the profession was founded, but traditional methods are slow and labour-intensive. The indiscriminate contagiousness of the virus meant few would be able to identify everyone they'd encountered (for example, in a crowded store or train). With so many people carrying smartphones, it was natural for governments to seek to exploit them even though there was no evidence that apps would be effective in the real world.[79] Two main types of contact tracing apps emerged: decentralised and centralised. In a decentralised system, each phone logs each phone it encounters and only uploads the log to a government server if the owner tests positive and gives consent. In a centralised system, those logs are constantly uploaded to a central store the government controls. In both cases, questions remain about how the data may later be used and whether citizens might be required to download and install the app and carry a phone at all times. To solve some of these issues, a group of academics led by Lilian Edwards proposed a safeguarding bill.[80] Another issue remained: what about the 22% of UK adults who have no smartphone?[81]

The pan-European Decentralised Privacy-Preserving Proximity Tracing sought to push governments to opt for the decentralised approach by creating an open source protocol that could underlie individual country's apps as a standard. Apple and Google also sought to aid interoperability by collaborating on a decentralised interoperable contact tracing platform.[82]

Many doubted that the apps would be effective.[83] Even in Singapore, with a high-tech population with great trust in the government, its open-source TraceTogether app was downloaded by only 13% of the population in its first week,[84] suggesting an even worse outcome for the UK, where experts estimated that to have an impact the app would have to be downloaded by 60% of the entire population, or 80% of smartphone owners.

In many countries, including the UK, quarantine enforcement was largely handed to law enforcement; in Britain police were granted extra powers to detain,

[79] "Contact tracing in the real world," by Ross Anderson, Light Blue Touchpaper, 2020-04-12: https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response.

[80] "The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates", by Lilian Edwards *et. Al*: https://osf.io/preprints/lawarxiv/yc6xu/.

[81] "Open Letter: Contact Tracking and NHSX", by Rachel Coldicutt, Medium, 2020-03-23: https://medium.com/@rachelcoldicutt/open-letter-contract-tracking-and-nhsx-e503325b2703.

[82] "How a handful of Apple and Google employees came together to help health official trace coronavirus", by Christina Farr, CNBC, 2020-04-28: https://www.cnbc.com/2020/04/28/apple-iphone-contact-tracing-how-it-came-together.html.

[83] "Track and trace or duck and dive - Covid19 surveillance apps", by Eva Pascoe, Cybersalon, 2020-04-14: http://cybersalon.org/track-and-trace-or-duck-and-dive-covid19-surveillance-apps.

[84] "Countries are using apps and data networks to keep tabs on the pandemic", *The Economist*, 2020-03-26: https://www.economist.com/briefing/2020/03/26/countries-are-using-apps-and-data-networks-to-keep-tabs-on-the-pandemic.

break up gatherings, and order people to go home. The early weeks of the UK lockdown were marked by actions many thought disproportionate: the Derbyshire police sent drones out in the Peak District to shame walkers[85]; and there were numerous reports of police violating social distancing guidelines to order people to move on in parks. The Northamptonshire police even threatened to investigate shopping carts to ensure people were not buying non-essential items, though they quickly followed up by denying that this was policy.[86]

Police were also granted the power to detain people suspected of being infected with COVID-19 who were not maintaining self-isolation for up to six weeks. By the end of April, police had issued 9,000 fines.[87] In other countries, lockdown and quarantine were more strictly enforced. In Azerbaijan, for example, residents under 65 were required to send text messages for permission to go out (those over 65 were not permitted out at all); in Kenya the authorities tracked the mobile phones of those suspected of being infected; and in Kazakhstan citizens under quarantine were required to install an app that used geofencing to alert the authorities if they left their designated area.

Also controversial were proposals for "immunity certificates" to allow people who had already been infected and recovered to return to normal life. The WHO warned that it was premature to consider immunity passports because it had not yet been proven that the presence of antibodies conferred immunity.[88] Others warned that the passports could become a vector for discrimination, and that requiring them in workplaces would encourage cheating and fraud.[89]

In China, citizens were required to install the Alipay Health app, which used myriad classes of data to score each individual's risk of being infected, which appeared on their phones as a green, yellow, or red code. These in turn determined where they were allowed to travel; the data was shared with law enforcement.[90] In addition, temperature checks were operated at the entrances to transport stations,

[85] "Coronavirus: Peak District drone police criticised for 'lockdown shaming'", BBC, 2020-03-27: https://www.bbc.co.uk/news/uk-england-derbyshire-52055201.

[86] "Coronavirus: Police backtrack after chief threatened to search shoppers' trolleys", by Richard Williams, Sky News, 2020-04-10: https://news.sky.com/story/coronavirus-police-backtrack-after-chief-threatened-to-search-shoppers-trolleys-11971269.

[87] "Coronavirus: More than 9.000 fines for lockdown breaches", BBC, 2020-04-30: https://www.bbc.co.uk/news/uk-52489943.

[88] "WHO warns against coronavirus immunity passports", by Emma Graham-Harrison, *The Guardian*, 2020-04-25: https://www.theguardian.com/world/2020/apr/25/who-warns-against-coronavirus-immunity-passports.

[89] "'Immunity Passports' Could Create a New Category of Privilege", by Emily Mullin, OneZero, 2020-04-23: https://onezero.medium.com/immunity-passports-could-create-a-new-category-of-privilege-2f70ce1b905

[90] "In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags", by Paul Mozur, Raymond Zhong, and Aaron Krolik, *New York Times*, 2020-03-01: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html.

public places, and workplaces, and even on buses[91]. How far such a system could be copied in Western countries was an open question; few believed the citizens of democracies would accept such invasive surveillance.

Many technology companies sought to embed their offerings at the heart of the pandemic response. AI and biometrics start-ups in numerous countries offered to donate their technology, and the Peter Thiel-founded data-mining company Palantir signed deals to build a platform to help track resources for the NHS[92] and, in the US, the Centers for Disease Control and Prevention. Also involved was the AI start-up Faculty, whose founder's brother had worked with Downing Street special advisor Dominic Cummings to build the Conservative party's private election data model.[93] NHS officials said the arrangement was temporary for the duration of the emergency.

The virus also spawned a wave of function creep, such as cameras that were claimed to be able to detect fever, sneezing, and coughing, and even social distancing. Many of these found their way into live experiments, such as the Connecticut town that trialled drones equipped with those expanded cameras in the belief that they could detect infected people in public parks. As of April 2020, it's a safe prediction that many of these technological fixes will prove useless.[94]

[91] "Guangzhou Deployes Biometric Tablets to Track Coronavirus on City Buses", by Nikkei Asian Review, *Find Biometrics*, 2020-03-30: https://findbiometrics.com/guangzhou-deploys-biometric-tablets-track-coronavirus-city-buses-033010/.

[92] "Palantir, a data firm loved by spooks, teams up with Britain's health service", *The Economist*, 2020-03-26: https://www.economist.com/britain/2020/03/26/palantir-a-data-firm-loved-by-spooks-teams-up-with-britains-health-service.

[93] "UK government using confidential patient data in coronavirus response", by Paul Lewis, David Conn, and David Pegg, *Guardian*, 2020-04-12: https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response,

[94] "Coronavirus News: Pandemic drones to monitor fever, crowds from above", by Dan Krauth, ABC News, 2020-03-15: https://abc7ny.com/coronavirus-drones-covid-19-pandemic-nj/6102905/.