Data Protection for Thrill Seekers

Dr Victoria Baines, IT Livery Company Professor of IT

19 March 2024

All hail the thrill seekers. The people who engage in extreme online activities like sharing personal information with others in order to receive their approval; who use apps to build emotional connections across the ether and enhance their physical pleasure; whose habits are formed by the quest for rewards and the dopamine hits associated with them;[1] who use technology to experience emotion, excitement, and an influx of feeling.

> *thrill, n. 1.a.*
>
> *A subtle nervous tremor caused by intense emotion or excitement (as pleasure, fear, etc.), producing a slight shudder or tingling through the body; a penetrating influx of feeling or emotion.*
>
> *Oxford English Dictionary*

Here's to the risk takers, who willingly expose themselves to the possibility of loss or injury; who fling their hard-earned cash through thin air; who broadcast their opinions; who tell potential burglars when they go off on holiday; who entrust their personal information to numerous people they have never met; who permit those same people to track their movements.

> *risk, n. 1.*
>
> *(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility. Frequently with of.*
>
> *Oxford English Dictionary*

There are now very few of us who have not done at least some of these things online. Indeed, I would go so far as to say that we are all digital thrill seekers and risk takers to some degree. Managing the risks we take in pursuit of our online thrills – whether these are an intimate relationship, unlocking a new level or experience in a game, likes for the content we share, or the purchase of a long-coveted items – entails securing their digital components. As users we are partly responsible for this, and there are measures we can take to improve both our security (who can have access to our accounts) and our privacy (what is shared).

By signing up to digital services such as social media and online retailers, we agree to their terms and conditions (Ts&Cs). We consent to them processing our personal data. It stands to reason, then, that service providers also have a responsibility to protect it. Data protection regimes and regulations enforce that responsibility. They also enshrine our rights as 'data subjects', the humans described by that data. Knowing and exercising our rights is not a trivial matter. But it *is* possible. This lecture explores how, and what is at stake.

Surveillance Capitalism

Our digital information is of value to a diverse ecosystem of service providers, retailers, and advertisers. When we supply our email addresses to an online retailer, this gives them a means to send us offers and updates. If they have my date of birth, they can tailor offers to my birthday. Retailers' marketing emails often

[1] http://www.theharvardbrain.com/fall-2020-nick-monaco.html

include pixels, HTML code that tracks when they are opened. They can also track when someone clicks through from the mail to their website. Search, social media and video sharing platforms store the content we share, but also data about the content we view, engage with, and search for.

Many flavours of online provider make extensive use of cookies, small text files that are downloaded onto your device when you visit a website. These can save you time by doing things like remembering what you have in your online shopping basket, or parts of pages to help them load faster. But they can also be used to track your browsing history, to gain insights into your interests and things you could be persuaded to purchase. This is the business model on which social media has thrived until recently. By learning more about our likes on their platforms, and our browsing habits off them, they can sell ads to brands on the premise that they can target them more effectively to people who are already in the market for a new car, raincoat, or guitar (for example). The process is similar to the one by which a service like Google monetises our web searches. The company sells ads that can be returned as sponsored search results when we search for a specific item or interest.

Online service providers would say that their Ts&Cs inform users on what handing over their personal data means, and that users have a choice whether or not to accept these. However, several international studies reveal that the vast majority of users do not read them: in one study by the European Commission (see Further Reading), as many as 90% of Brits and the same proportion of Europeans on average accepted the Ts&Cs, but only 21% reported that they had read them in full. In the US, just 9% reported that they always read a company's privacy policy before agreeing to the terms.[2] One reason for this appears to be the density of the policies. In 2020, digital bank thinkmoney compared the word counts of the Ts&Cs for thirteen of the most popular apps in the UK.[3] These ranged from just under 5,000 words for Google Meet to over 18,000 words for Microsoft Teams. The total word count for the apps reviewed came to 128,415 – longer than most PhD theses, mine included.

If we were minded to be cynical, we might argue that it's in online providers' interests not to have too many users enforcing their rights to opt out. Legally and technically speaking, cookies do not log any personal data of the kind that could be used by themselves to identify us. But they do allow for capture of information that we as individuals may have thought was personal to us because it reflects our passing thoughts, the contents of our heads at a particular time.

There are things we can do to stop this kind of tracking and profiling. They require a certain amount of effort on our part. We can unsubscribe from marketing emails that we no longer want to receive. We can send providers a clear instruction to delete our contact details from their databases. We can opt out of all but the strictly necessary cookies. If we continue to Accept All, legally consenting to not only essential, but also functional, performance, and marketing cookies, we should at least be able to satisfy ourselves that we have done so consciously, and not through ignorance or laziness.

Less visible are the data brokers, companies who scrape our data, often from publicly available sources like the electoral register and pages on the open web, and then combine it in lists that they then sell on for marketing. These include Credit Reference Agencies like Experian, Equifax, and TransUnion. An investigation by the UK Information Commissioner's Office (ICO) found that agencies were not sufficiently transparent with consumers about how their data would be used when they performed credit checks and identified several other areas of concern.[4] As a result, all three companies named above were served with preliminary enforcement notices. This led to Equifax and TransUnion making improvements and even withdrawing certain products and services.

Knowing Your Rights

As you may remember if you listened to my lecture on encryption last year,[5] privacy is a human right, enshrined in Article 12 of the *Universal Declaration of Human Rights* proclaimed by the United Nations General Assembly in 1948. In 2018, the UN's High Commissioner for Human Rights published a report on

[2] https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/
[3] https://www.thinkmoney.co.uk/blog/what-phones-know-about-you/
[4] https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf
[5] https://www.gresham.ac.uk/watch-now/problem-encryption

the right to privacy in the digital age (A/HRC/39/29), which urged states to implement laws and institutions for the protection of personal data.[6] In 2021, the UN Conference on Trade and Development (UNCTAD) found that 137 out of 194 countries had put such legislation in place.[7]

Foremost among these has been the EU's General Data Protection Regulation (GDPR), which came into force in May 2018. This applies to any organisation that processes the data of EU citizens, wherever it may be located. For now, at least, it is still in force in the UK because it was adopted before the UK left the EU. Data protection is a fundamental right as set out in Article 8 of the EU Charter of Fundamental Rights. Accordingly, GDPR sets out our rights as data subjects. Chief among these are:

- The right to clear and transparent information on the processing of personal data, whether or not it has been obtained directly from us (Transparency, Articles 12, 13, & 14)
- The right to obtain a copy of any personal data held on us via a Subject Access Request (Right of Access, Article 15)
- The right to have inaccurate personal data corrected (Right to Rectification, Articles 16 & 19)
- The right to have data erased where certain conditions are met ('Right to Be Forgotten, Articles 17 & 19)
- The right to obtain portable data for re-use in another context (Right to Data Portability, Article 20)
- The right to object to processing of our personal data where this is in connection with tasks carried out in the public interest, in the exercise of official authority, in the legitimate interests of others, or for the purpose of direct marketing (Article 21)
- The right not to be subject to a decision based solely on automated processing or automated profiling (Article 22)

These read as powerful means to hold data controllers accountable, and especially online providers that process large amounts of our personal data. In practice, this requires each of us to contact the provider directly whenever we want to exercise our data protection rights. The data controller must respond within one month, unless they can demonstrate that they need an extension or there is no merit in the request (Article 12). If the request is not answered to their satisfaction, individuals in the 28 EU Member States as they were in 2018 can complain to their national Data Protection Authority, whose establishment is also required under GDPR (Articles 51 to 59). These authorities have the power to fine data controllers, also if it is demonstrated that they have not acted in accordance with the principles (Article 5) of lawfulness, fairness, and transparency; accuracy, accountability, integrity and confidentiality; or that they have not limited the purpose for which they collect data, minimised the data collected, or limited the time for which it is stored.

Fines can be as large as 20 million Euros, or 4% of total annual turnover for infringements of individuals' rights above, whichever is the higher. For companies like Google and Microsoft, with respective annual turnovers of over 300 billion USD and over 200 billion USD, this is no mean sum. Fines do happen. In May 2023, Meta (formerly Facebook) was fined 1.2 billion Euros by the Irish Data Protection Commission for transferring the personal data of European users to the US without adequate data protection mechanisms. In 2021, the Data Protection Commission in Luxembourg fined Amazon 746 million Euros for targeting ads at people without proper consent. In this case, the complaint was filed by 10,000 people through French privacy rights organisation La Quadrature du Net. For the time being, at least, fines issued by national regulators are transferred to government treasuries, not to the individuals affected.

Data Activism

Objecting to online services' Terms and Conditions (Ts&Cs) can sometimes be easier said than done. Accepting provider policies is the path of least resistance, the practical alternative to which is often walking away. Very rarely do we have the option to accept some terms and reject others. On services like search engines and social media, rejecting the terms may mean disenfranchisement: having access to less information than other people, or being isolated from our peer networks. When our use of IT is so essential to knowledge acquisition and community building, the choice is in fact no choice at all.

A lack of meaningful consent is just one of the issues on which Max Schrems, an Austrian lawyer and privacy activist, has campaigned. Challenging the assumption that one human can do nothing to stop Big Tech companies in their tracks, between 2011 and 2013 Schrems filed a total of 22 complaints with the Irish Data

[6] https://documents.un.org/doc/undoc/gen/g18/239/58/pdf/g1823958.pdf?token=ECONsCcxWGv0GCwIkc&fe=true
[7] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Protection Commissioner about the operations and policies of Facebook Ireland Ltd, the company's European data controller.[8] The last of these concerned the export of European users' data to the US in light of claims by Edward Snowden that the PRISM surveillance programme enabled the US National Security Agency to access this data. This eventually led to the European Court of Justice declaring the legal basis for these transfers invalid, which in turn meant that the EU and the US had to agree a new framework for transatlantic data transfers.[9]

Activists have sought also to bring civil lawsuits against Big Tech companies, with the promise of compensation for those affected. In 2014, Max Schrems was joined by 25,000 other users in a 'class action' lawsuit against Facebook, seeking a token amount of 500 Euros per user for privacy violations. Initially dismissed by the Vienna District Court, this ruling was overturned by the Vienna's Higher Regional Court. In 2018, the collective action was dismissed by the European Court of Justice. But in 2021 the Austrian Supreme Court ruled that Schrems should be awarded the 500 Euros he was seeking for himself and referred the case back to the European Court.

In 2023, Meta agreed to pay 725 million USD to settle a legal action on behalf of 87 million users whose data was allegedly shared without their consent with third parties including British company Cambridge Analytica. Anyone in the US who used Facebook between 2007 and 2022 can now claim a share of that compensation. And in February 2024 a judge in the UK gave the go-ahead to collective proceedings brought by Dr Liza Lovdahl Gormsen on behalf of millions of users who had Facebook accounts between February 2016 and October 2023, seeking compensation of between £2.07 billion and £3.1 billion. The application has been made to the Competition Appeal Tribunal on the basis of alleged anti-competitive behaviour. Its claim that "Facebook has struck an unfair bargain with its users in relation to its collection of data from users on their activities outside of Facebook" highlights the criticality of our personal data to the success of Big Tech business models.[10] It prompts the question, if we are contributing to this success, where are our dividends?

Very Personal Data

In my lectures on the Massive Internet of Things and Brain Computer Interfaces, we considered how an ever-increasing number of connected devices generate, process, and store medically sensitive data, and how these are quite often controlled by private companies.[11] GDPR puts additional conditions on the processing of special categories of personal data that are deemed to be more sensitive (Article 9), concerning:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data
- A person's health
- A person's sex life
- A person's sexual orientation

There are separate provisions for data on criminal offences (Article 10). Processing of special category personal data is prohibited unless one of the following applies:

(a) The data subject has given explicit consent
(b) It is necessary to fulfil obligations of employment, social security and social protection (if authorised by law)
(c) It is necessary to protect someone's vital interests
(d) It is carried out by a not-for-profit body with a legitimate interest

[8] http://europe-v-facebook.org/EN/Complaints/complaints.html

[9] https://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddbb8c0c2b301a4ad08e2d83c41bc63c36.e34KaxiLc3qMb40Rch0SaxuRbxb0?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=253155

[10] Competition Appeal Tribunal Case No. 1433/7/7/22, available at https://facebookclaim.co.uk/media/ppab0ndv/cpo-application-and-hearing-notice.pdf

[11] https://www.gresham.ac.uk/watch-now/massive-internet; https://www.gresham.ac.uk/watch-now/brain-computer

(e) The data subject has made it public
(f) It is necessary for due legal or judicial process
(g) It is necessary due to substantial public interest (with a basis in law)
(h) It is necessary for the delivery of health or social care (with a basis in law)
(i) It is necessary for public health (with a basis in law)
(j) It is necessary for archiving in the public interest, research and statistics (with a basis in law)

These protections are in addition to all the principles and individual rights set out in GDPR. The special category provisions do not, however, oblige providers to protect medically or otherwise sensitive data with additional security.

In our daily lives we share this more sensitive kind of personal data with private companies much more frequently than we might realise. If we use one of a plethora of apps to help us with our mental health – whether that is self-help such as guided meditation or journalling, or to connect with therapists – we routinely share health-related personal data. Apple Health allows users to generate a 'medical ID' complete with blood type, allergies, medical conditions, and medications for sharing with emergency responders. Apple Health and Fitbit (owned by Google) enable menstruating users to track their cycles.

Researchers at civil society organisations Privacy International and Coding Rights discovered that several period tracking apps encouraged users to log additional lifestyle information, including when, how, and how often they have sex, and their birth control habits.[12] Moreover, Privacy International found that some of these apps were sharing data with third parties, including Facebook (now Meta).[13] As well as being special category data under GDPR, this kind of data is being viewed in a new light since in 2022 the US Supreme Court overturned the legal ruling that a woman's right to terminate her own pregnancy was protected by the US Constitution (Roe v. Wade). In US states where abortion is illegal, law enforcement can compel providers such as online pharmacies and social media platforms to disclose user data relevant to criminal investigations. As research by ProPublica has found, some online pharmacies that retail abortion pills share data with Google that can potentially identify them, which could then be requested from Google by the authorities.[14] Even before Roe v. Wade was overturned, Meta reportedly disclosed the private messages of a 17-year-old girl and her mother facing criminal charges in Nebraska for carrying out an abortion after 20 weeks of pregnancy. In this case, the content sought was on Facebook Messenger, not a third-party app, and the investigators served a search warrant on the company.[15]

In the previous lecture, Sex and the Internet, we looked briefly at the 2015 hack of dating site Ashley Madison, known for connecting people who want to have affairs.[16] The hackers threatened to publish the personal data of users, including their real names, home addresses, and credit card payments. They claimed to be motivated by moral outrage at the unethical practices of the platform. They demanded the immediate closure of the service, and when this didn't happen within a month they published the data of millions of users. Among them were users who had paid Ashley Madison's parent company to close their accounts and delete their personal information. Their appearance in the stolen data sets suggested that the platform had retained the personal data even of those people who had paid them not to.[17] This breach happened before GDPR came into force in the EU. Under the current regime, the company potentially would have failed to meet individuals' right to be forgotten (Article 17 & 19).

The Data That Makes Us 'Us'

Millions of us have shared our genetic data with private companies by taking DNA tests: 14 million with

[12] https://chupadados.codingrights.org/en/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros-2/
[13] https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data
[14] https://www.propublica.org/article/websites-selling-abortion-pills-share-sensitive-data-with-google
[15] A copy of the affidavit for the search warrant can be viewed at https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion?utm_source=motherboard_twitter [WARNING: CONTAINS MATERIAL THAT YOU MAY FIND DISTRESSING].
[16] https://www.gresham.ac.uk/watch-now/internet-sex
[17] https://www.theguardian.com/technology/2015/aug/19/ashley-madisons-paid-delete-option-left-data-identifying-users-post-claims

23andMe, and over 25 million with Ancestry DNA.[18] Consumer genotyping opens up the possibility to profile our dispositions to certain health conditions and gives us insights into our heritage. Some users have discovered their birth parents and other close relatives purely through permitting an online provider to perform this analysis. In 2015, researchers at Princeton's Center for Information and Technology Policy noticed that Ancestry.com's privacy policy gave the company permission to use its customers' genetic information for advertising purposes.[19]

Ancestry.com has since clarified that it does not share individuals' data sets with advertisers and has changed its privacy policy to exclude advertising from its description of how it uses genetic information. However, they do still state that they share with marketing and advertising partners 'inferences', "derived from personal information, such as to suggest familial relationships and to create consumer profiles for the purposes of research, product development and marketing", examples of which include "your ethnicity estimate, traits, and Genetic Communities".[20] The company describes the last of these as "groups of AncestryDNA members who are connected through DNA most likely because they descend from a population of common ancestors".[21] So, those of us who take their tests seem to have agreed, albeit tacitly and perhaps unwittingly, to being served online ads on the basis of our genetic make-up.

It can be difficult – and arguably disingenuous – to disentangle data protection from cybersecurity. If data is secure, it is better protected. In December 2023, 23andMe confirmed that hackers had stolen ancestry data on 6.9 million users.[22] In a letter sent to a group of victims, the company's lawyers stated that "the incident was a result of users' failure to safeguard their own account credentials, for which 23andMe bears no responsibility."[23] The hackers appear to have re-used compromised login credentials for other services and gained access to users' accounts where they had used the same password across a number of platforms – a type of attack known as 'credential stuffing.' But they didn't do this 6.9 million times. They compromised 14,000 accounts. Because of the way the platform works, they were able to gain access also to the personal information of customers who had automatically shared data with their hacked DNA relatives.[24] 23andMe responded by resetting all user passwords and requiring everyone to use multi-factor authentication (MFA). Had the latter been obligatory before the incident, it's possible that far fewer accounts would have been compromised. Equally, one could argue that the company has a duty/responsibility to 'air gap' user data, shutting off linked data for relatives where there are indications of account compromise, such as logins from an unexpected location or device.

According to GDPR, our faces are also personal data. In this context, the increasing use of live, automated facial recognition has proved not only to be controversial but often contravening. It is the opinion of the UK Information Commissioner's Office (ICO) that its use by law enforcement is incompatible with the right to respect for a private life under Article 8 of the European Convention on Human Rights and data protection legislation.[25] Of particular concern is the practice of scanning people's faces and processing of their personal data without their knowledge or consent. In a high-profile case in 2020, a court heard that South Wales police had captured 500,000 faces, "the overwhelming majority of whom were not suspected of any wrongdoing."[26] Online, companies like Clearview AI that scrape billions of publicly available images of people's faces – again without their knowledge or consent – for processing by law enforcement are now coming under increasing scrutiny by national regulators.[27]

[18] https://medical.23andme.com/; https://support.ancestry.com/s/article/About-AncestryDNA?language=en_US
[19] https://freedom-to-tinker.com/2015/09/07/ancestry-com-can-use-your-dna-to-target-ads/
[20] https://www.ancestry.com/c/legal/privacystatement?_gl=1*1wx3alp*_ga*MTQ5OTU2NTUyNS4xNzA5NTQ2MjM1*_up*MQ..#shared-info
[21] https://support.ancestry.co.uk/s/article/How-are-DNA-communities-used-in-my-Origins-results
[22] https://techcrunch.com/2023/12/04/23andme-confirms-hackers-stole-ancestry-data-on-6-9-million-users/
[23] https://www.documentcloud.org/documents/24252535-response-letter-to-tycko-zavareei-llp
[24] https://techcrunch.com/2024/01/03/23andme-tells-victims-its-their-fault-that-their-data-was-breached/?guccounter=1
[25] https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf
[26] https://www.theguardian.com/technology/2020/aug/11/south-wales-police-lose-landmark-facial-recognition-case
[27] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/11/information-commissioner-seeks-permission-to-appeal-clearview-ai-inc-ruling/

Whose Rules?

When so much of our very personal and sensitive data can be processed and stored internationally, it makes sense for data governance regimes to be international, or at least approximate, so that each of us can be assured that we can expect our data to be handled to similar standards in different countries. One of the reasons why GDPR is held up as the gold standard of data protection is that it applies to everyone who wants to process the personal data of EU citizens, wherever that processor may be located, and it required the 28 Member States in 2018 (and those in the European Economic Area) to introduce the same level of legal protections.

Seen through this lens, the UK government's introduction of new legislation in the form of the Data Protection and Digital Information Bill may be viewed as an expensive attempt to reinvent the wheel in a post-Brexit flexing of national sovereignty. One of the publicised promises of the Bill is that it will reduce the number of "annoying cookie pop ups" we see.[28] Annoying they may be, but we may rightly feel that receiving fewer opportunities to exercise our right to object to being profiled through our online browsing habits is not the most just solution. While the intention may be to give the consumer a more convenient experience, this should not be at the expense of their right to control how their personal data is collected and processed. Personally, I would prefer to have the opportunity to consent or reject *every time* that data is requested. The alternative of a one-time, blanket consent can open up opportunities for organisations to use data in ways that subjects may not have originally intended.

Scrutiny by regulators intensifies whenever Big Tech companies seek to acquire smaller providers. When Facebook (now Meta) bought WhatsApp in 2014, it informed the European Commission that it would not be able to conduct reliable automated matches between Facebook users' accounts and WhatsApp users' accounts, thereby joining the two datasets together and enabling deeper insights into users' lives and behaviours. In 2016, however, WhatsApp updated its terms of service and privacy policy, and included the possibility of linking WhatsApp users' phone numbers to Facebook accounts. As a result, the EU fined Facebook 110 million Euros for providing incorrect information during the investigation of the merger.[29]

Those of us who wear an Apple Watch are used to the idea that data is shared with our other Apple devices. If you own a rival Fitbit tracker, you may not know that Google now owns Fitbit - and therefore has access to your health and fitness data. Originally announced in 2019, the acquisition was completed in 2021 following a European Commission investigation. While the chief focus was on whether Google's access to Fitbit users' health and fitness data would give their advertising business an unfair advantage over competitors, both Google and Fitbit were quick to reassure the public that Fitbit data would not be used to target Google ads at them.[30] Had the EU not explicitly banned this, this safeguard might not have been put in place.

Data captured by connected devices in our homes is processed by providers and sometimes shared across services. As the owner of both Ring doorbell and Alexa/Echo smart speaker technologies, Amazon processes video recordings of users' properties and uses voice recordings to train its speech recognition and natural language understanding systems.[31] Smart home device data is also of increasing interest to law enforcement authorities.[32]

Exercising Our Rights

Enforcement of our data rights relies on several groups of people who act in our interests: investigative journalists such as Carole Cadwalladr, who first exposed that the data of millions of Facebook users had been collected by consulting firm Cambridge Analytica without their consent;[33] activists like Max Schrems, who have made it their mission to pursue alleged infringements against themselves and others; civil society organisations, particularly those focused on privacy, surveillance, and freedoms of expression and information; and state, national and international regulators.

---

[28] https://www.gov.uk/government/news/new-data-laws-debated-in-parliament
[29] https://ec.europa.eu/commission/presscorner/detail/pl/IP_17_1369
[30] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2484
[31] https://www.bbc.co.uk/news/technology-51709247;
https://www.amazon.co.uk/gp/help/customer/display.html?nodeId=GVP69FUJ48X9DK8V
[32] https://www.wired.com/story/star-witness-your-smart-speaker/
[33] https://www.theguardian.com/news/series/cambridge-analytica-files

But if the data is ours, how can we get greater control over it? Think tank Demos, law firm Schillings, and consumer data action service Rightly conducted research on users' experiences of trying to reclaim their personal data.[34] One of the key findings of their report is that the data collected and inferred about users online goes beyond their expectations. Some platforms, such as those provided by Meta, give users the option of downloading a copy of their account and usage data.[35] I have yet to meet anyone who has reviewed their downloaded data and not been surprised by the amount and the level of detail they saw.

In addition to the expected likes, direct messages, posts, photos, group membership, logins and GPS location data, information can include what TV and movies you watch and when, the news sources you read, the websites you visit, and logins for other apps and services, where you have given permission for these to be linked to your social media. Also available to view is a list of advertisers that have included you in their audience based on existing mailing lists or interactions with their websites, apps, or stores. Platforms make inferences about us, putting us in groups that are then used to target advertising, and these can be quite revealing. I, for instance, am characterised as 'Away from family', 'away from home town', 'Facebook page admin', 'early technology adopter', and 'frequent international traveller' – all of which have been true at some point in the life of my account but are not necessarily completely up to date. Once you know what is being collected and shared, you can take steps to restrict that, should you so wish. A good place to start is Facebook's Privacy Checkup tool.[36]

Rightly Protect is one of several free tools that can help you find out which companies have your data and send an automated request for them to erase it when you no longer want them to have it. It analyses your email inbox to do this, which may feel a little counterintuitive from a security standpoint. But for the most part, the expectation is that consumers will gather information from organisations on the data they hold. As with Subject Access Requests under GDPR, the onus is on us to proactively investigate and then stop companies in their tracks. If we had the chance to do this all again, would we design the global data ecosystem differently, so that humans could have greater control over their own personal information?

The inventor of the world wide web, Tim Berners-Lee, thought as much when in 2016 he established Solid (Social Linked Data), a project intended to give individual users full control over the usage of their personal data.[37] Solid is a protocol that allows data to be stored securely in decentralized web servers called pods. Pod owners control which people and applications can access the data, meaning it's a user-centric – rather than a company-centric – model for data protection. So far, however, the project hasn't taken off, despite considerable media and public interest in the wake of major data mishandling scandals. This could be due to the level of technical skill required to run a pod server, restricting uptake largely to developers. A user-friendly solution for consumers is yet to emerge, and it's still uncertain whether pod providers will charge for the service.

For the time being, at least, there are no shortcuts for those of us wanting to exercise our rights over how our personal data is collected, processed, and stored. In the trade-off between privacy and convenience, it's up to each of us to decide how comfortable we are with sharing our personal information with tech companies and other online service providers. This in turn relies on us being properly informed, which can be time consuming. But it's too important for us to sleepwalk through. One day, your financial security, your reputation, and even your physical safety could depend on it.

Resources

Knowing your rights

National data protection authorities often have clear and accessible information on individuals' data rights. In addition to investigating and enforcing against possible infringements, the UK Information Commissioner's Office (ICO) publishes guidance for data controllers and processors, but also these pages on our rights as data subjects:

https://ico.org.uk/global/privacy-notice/your-data-protection-rights/

The EU's 'one stop shop' regulator for several Big Tech companies, the Irish Data Protection Commissioner's

[34] https://demos.co.uk/wp-content/uploads/2023/04/accept-all-unacceptable-demos-march-2023.pdf
[35] https://www.facebook.com/help/212802592074644
[36] https://www.facebook.com/help/443357099140264
[37] https://solidproject.org

(IDPC) website includes some useful resources for consumers. Its guide to *Data Protection Basics* is particularly good:

https://www.dataprotection.ie/sites/default/files/uploads/2019-07/190710%20Data%20Protection%20Basics.pdf

Exercising your rights

National data protection authorities can also be good starting points for finding out what data providers hold on you. The UK ICO provides a service which submits subject access requests to organisations on your behalf: https://ico.org.uk/global/privacy-notice/using-our-subject-access-request-service/

If you're unsure which organisations to address, free tools like Rightly Protect can help. You *do* need to give permission for the tool to analyse some data from your email inbox. It identifies mailing lists to which you have subscribed, and sends automated requests for your data to be erased by services you no longer use: https://right.ly/rightly-protect/

Some (but not all) online service providers provide 'self-serve' tools for you to access some (but not always all) of the data you generate on their platforms. Here is a selection for the most popular platforms:

- Meta (Facebook, Instagram, WhatsApp) – https://www.facebook.com/help/212802592074644
- Google (includes YouTube) – https://support.google.com/accounts/answer/3024190?hl=en
- Microsoft – https://account.microsoft.com/privacy
- Apple – https://support.apple.com/en-gb/102283
- Amazon – https://www.amazon.co.uk/hz/privacy-central/data-requests/preview.html

Last but not least, None Of Your Business (NOYB) is the civil society organisation founded by Max Schrems. Its website contains step-by-step guides to exercising each of the eight GDPR rights for individuals: https://noyb.eu/en/exercise-your-rights

Further Reading

Baines, V. (2021), *On Joined Up Law-making: The Privacy/Safety/Security Dynamic, and What this Means for Data Governance*. SSRN: https://ssrn.com/abstract=3958982

Demos (2023) *Accept All: Unacceptable? Tracking the experience of trying to reclaim personal data – and what government, businesses and citizens can learn from it*. https://demos.co.uk/wp-content/uploads/2023/04/accept-all-unacceptable-demos-march-2023.pdf

European Commission, Consumers, Health, Agriculture and Food Executive Agency, Elshout, M., Elsen, M., Leenheer, J. et al. (2016), *Study on consumers' attitudes towards Terms and Conditions (T&Cs) – Final report*, Publications Office of the European Union, https://data.europa.eu/doi/10.2818/950733

Zuboff, S. (2018) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* Profile Books.