DEMOS

ACCEPT ALL: UNACCEPTABLE?

TRACKING THE EXPERIENCE OF TRYING TO RECLAIM PERSONAL DATA - AND WHAT GOVERNMENT, BUSINESSES AND CITIZENS CAN LEARN FROM IT

ELLEN JUDSON
VICTORIA BAINES

MARCH 2023

SCHILLINGS

RIGHT (1)

This project is in partnership with Schillings.
The research was supported by our project partner Rightly.

Published by Demos March 2023

15 Whitehall, London, SW1A 2DD
T: 020 3878 3955
hello@demos.co.uk
www.demos.co.uk

CONTENTS

ACKNOWLEDGEMENTS **PAGE 4**

EXECUTIVE SUMMARY **PAGE 5**

KEY RESEARCH FINDINGS **PAGE 7**

POLICY RECOMMENDATIONS **PAGE 9**

PART ONE: TRACKING DOWN YOUR DATA **PAGE 11**

- **METHODOLOGY** **PAGE 11**
- **ONLINE IDENTITY:** HOW ONLINE SYSTEMS CREATE IDENTITIES FOR YOU THAT YOU ARE UNAWARE OF **PAGE 14**
- **THE BIG LIE:** HOW PROCESSES MEANT TO EMPOWER USERS TO BE IN CONTROL OF THEIR DATA DO THE OPPOSITE **PAGE 20**

PART TWO: FUTURE POLICY SHAPING **PAGE 26**

- **DIGITAL ACTORS:** WHO CAN MAKE CHANGE HAPPEN? **PAGE 27**
- **CURRENT POLICY:** THE STATUS QUO **PAGE 29**
- **THE WAYS FORWARD:** ROUND TABLE RECOMMENDATIONS **PAGE 30**
- **THE FUTURE:** A NEW STORY FOR PRIVACY **PAGE 31**

CONCLUSION **PAGE 36**

APPENDIX **PAGE 37**

ACKNOWLEDGEMENTS

Huge thanks must go to all of our partners with whom we've collaborated on this project, without whom this report would not have been possible!

Firstly, thanks must go to Annie Scott, Nigel Higgins, Angharad Mountford, Christopher Mills, Tori Clarke and the whole team at Schillings for supporting this project and for all their work throughout.

Thanks also to James Walker, Beatrice Farina and Jane Henry at Rightly for leading the data investigations with our volunteers; Will Nicholson and Neil Edwards at TVN for their work on the documentary that accompanied this project; and Demos colleagues past and present, in particular Alex Krasodomski-Jones, Felix Arbenz-Caines, Charlotte Campbell-Nieves, Ciaran Cummins, Polly Curtis, Alice Dawson, Kosta Juri, Sophia Knight, Jon Nash, Josh Smith, Selina Swift,and Maeve Thompson.

And of course thanks must go to all of our research participants, for sharing their time and experiences with us and helping us investigate the current problems facing people in taking control of their data, as well as those who participated in our policy roundtables to help shape the recommendations for a path forward.

As ever, any errors or omissions are the authors' own.

Ellen Judson

March 2023

EXECUTIVE SUMMARY

This project, a collaboration between Demos, the law firm Schillings and the independent consumer data action service Rightly, seeks to investigate how our data footprints are being created and exploited online.

Data is the bedrock of the digital economy. Companies are increasingly competing to generate and have access to as much data about us as possible, crafting the digital environment and their products around the insights large datasets give. Other companies facilitate and profit from this, building entire business models from the collection and sale of this precious data. User privacy, protecting people's personal data and information from abuse or exploitation, comes secondary to enabling more effective advertising and targeting. Existing data regulation gives more powers to users, but too often this is not translating into actual insight or control over their personal data.

For its advocates, the data economy offers unparalleled opportunities for tailoring and designing services and products around the needs and desires of their users. For its detractors, 'surveillance capitalism' - as it was famously termed by Shoshana Zuboff - has come to embody a system in which users have significantly *less* power, treated as data points from which information can be extracted and exploited for profit.[1]

Multiple actors swirl around our data. Social media platforms are notorious for being advertising platforms that collect information about every click and scroll to precisely target us. Online shops become reliant on that social media data, tracking customers through their stores then using platforms to target those same customers with items they had recently viewed. Meanwhile, insurance companies collect personal data to make estimates about who we are and the lives we live to price policies. Data brokers scrape information about all of us from publicly available data on the internet, that other companies are then able to buy, in a practice widely critiqued due to lack of fairness, transparency and knowledge amongst the public that this practice even occurs.[2]

As knowledge and outcry about these practices has grown, so too have regulatory responses. Governments, international bodies (like the EU) and regulatory bodies (like the UK's Information Commissioner's Office (ICO)) are now important players in the data economy.

Then there are the individual internet users - you and I. We each leave trails of data as we navigate webpages, clicking cookie banners and logging into different services via social media accounts. Increasingly, members of the British public are unconcerned about where their data goes[3]: perhaps due to the convenience of free services their data enables, or the invisibility of how their data is actually being used.

1 Zuboff, Shoshana. *The Age of Surveillance Capitalism*.
2 ICO. Data Brokering: Understanding the public's perception of the sharing of their personal details. No Date. Available at: https://ico.org.uk/media/for-organisations/documents/2618466/ico-data-brokers-research-presentation-2903191.pdf [last accessed 09/02/23]
3 Data & Marketing Association. UK Data Privacy: What the consumer really thinks. 2022. Available at: https://dma.org.uk/uploads/misc/dma---uk-data-privacy-2022.pdf [last accessed 09/02/23]

The competing interests of these actors mean that behind cookie banners are high-stakes debates. Data collection is how many websites are able to make money that might otherwise place content behind paywalls, creating a trade-off between privacy rights and the accessibility of the online world.[4] There are many who wish to disrupt this status quo. Some disrupt through technical means, using new technologies like data pods or blockchain to increase the visibility of data transfers and user control.[5] Others wish to reverse the logic of the market entirely and want users to be paid for the use of their data by those that profit from it.[6] Meanwhile, the UK has positioned the EU's GDPR as a barrier to science and business innovations because of the compliance burden, and want to institute data reforms that would "unlock [its] power",[7] while maintaining data adequacy with the EU. Civil society groups warn this move would make users vulnerable to greater online manipulation through micro-targeting and surveillance.[8]

We carried out an exploratory investigation into how data sharing and data regulation practices are impacting citizens: looking into how individuals' data footprints are created, what people experience when they want to exercise their data rights, and how they feel about how their data is being used. This was a novel approach, using live case studies as they embarked on a data odyssey in order to understand, in real time, the data challenge people face.

We then held a series of stakeholder roundtables with academics, lawyers, technologists, people working in industry and civil society, which focused on diagnosing the problems and what potential solutions already look like, or could look like in the future, across multiple stakeholder groups.

You can watch a documentary produced by the project partners and TVN, alongside this report, here.

4 Cummins, Ciaran and Victoria Baines. The Cost of Creation: What is a Fair and Desirable Future for Monetised Online Work and Volunteering. Demos. 2022. Available at: https://demos.co.uk/project/the-costs-of-creation-what-is-a-fair-and-desirable-future-for-monetised-online-work-and-volunteering/ [last accessed 09/02/23]

5 Solid Project. Available at: https://solidproject.org/ [last accessed: 09/02/23]

6 Data Dividend Project. Available at: www.datadividendproject.com/ [last accessed: 09/02/23]

7 DCMS. New data laws to boost British business, protect consumers and seize the benefits of Brexit. 2022. Available at: www.gov.uk/government/news/new-data-laws-to-boost-british-business-protect-consumers-and-seize-the-benefits-of-brexit [last accessed 09/02/23]

8 Big Brother Watch. Response to Data Law 'Reform' Plans. 2022. Available at: https://bigbrotherwatch.org.uk/2022/06/response-to-data-law-reform-plans/ [last accessed 09/02/23]

KEY RESEARCH FINDINGS

Our research investigated the experiences of five volunteers as they attempted to understand who had their data, exactly what data they had and what happened when they tried to have that data deleted. The volunteers expected the information held on them to be minimal and restricted to information such as name, date of birth and address. Instead, the data collected and inferred about users goes far beyond this. The process of trying to take control of your data is complicated, time-consuming, and no guarantee of success. The systems and processes can sometimes work - but there are huge limitations for individuals trying to exercise their data rights and compliance is far from always clear and consistent.

The data collected and inferred about users goes far beyond what data people are expecting is held on them

The data collected about users online can be both extremely wide-ranging, and extremely granular and precise. Our volunteers found a huge variety of personal data about themselves kept by companies - from extensive histories of how they interacted with a company or website, to location and financial histories.

Using one website or application is just one point in a chain of companies collecting and buying your data. There can be hundreds or even thousands of different companies which are using your data to target advertising

Even using just one service led to data on our volunteers being shared further with a huge network of companies, to target them based on their interests, from recruitment to marketing to shopping services.

Your data footprint includes wide-ranging assumptions about your characteristics, identity and how you are likely to act in the future: information which is sold on to enable more effective marketing

Personal data isn't limited to information you have directly shared with a company: information held on you can include 'propensities' - from what kind of movies you like, where you read the news, what you like to do in your spare time, how much money you are likely to spend on certain things. This may not always be accurate, but can affect what products and services are targeted or available to you.

"There's information about me out there, that I don't know what people are doing with".

Trying to take control of your data is complicated, time-consuming, and no guarantee of success. The systems and processes can work - but there are huge limitations for individuals trying to exercise their data rights. The process is complex and requires a great deal from the user

Although sending data requests to companies was supported by the Rightly Protect service, this was still a heavily involved process for our volunteers. Volunteers were often asked by companies to provide more personal information, follow up with different departments, or use self-service data portals: with different systems and response rates and types from the numerous different companies that held information on our volunteers.

Data requests are often complied withm, but this isn't happening clearly or consistently. Often companies are not even able to delete user data upon request, due to other legal requirements

There is good practice: there were timely, relevant responses from companies. But it was not consistent. For some volunteers, 65% of their data requests were responded to; while for others, only 10% of their data requests to companies were answered. And replies themselves did not guarantee data would be deleted: indeed, they sometimes resulted in a refusal to delete data, citing their existing policies or compliance obligations.

"It's a job in and of itself, you have to manage each one, see when they respond."

As the UK government seeks to reform how data is processed and protected in the UK, we hope this report will be a call for citizens' data rights to be at the heart of those reforms.

POLICY RECOMMENDATIONS

Business	Improving the short term	Adopting new ad-tech solutions that drastically reduce the amount of tracking and data collection required
		Incorporating privacy-by-design
		Assessing where data is likely to be collected on children and developing safeguards to reduce the amount of data collected on children
		Develop more easily accessible terms of service
	A long-term vision for data privacy	Invest in developing and deploying privacy-preserving infrastructure

Governments	Improving the short term	Stronger, clearer and more easily accessible enforcement mechanisms for privacy violations, including enforcement of the UK GDPR
		Public education campaigns and supporting greater digital literacy education in order to promote understanding of online privacy
		Developing standards for privacy architecture, improving the user experience of interventions such as cookie banners
		Developing standards and a process for researcher access to data
		Develop minimum standards and guidance for how companies seeking to comply with regulation can do so in a privacy-preserving way
		Protect simple ways that users can protect themselves online like end-to-end encryption and VPN
	A long-term vision for data privacy	Tackle surveillance advertising model through regulation similar to the Digital Services Act
		Use the forthcoming Digital Markets regulation as another vehicle for challenging the tech monopolies
		Use the opportunity of the new Data Reform Bill to ensure strong data protection regulation that centres the needs of citizens
		Use regulation to improve the transparency and accountability of AI and the algorithms used to process and analyse the vast quantities of data collected
Collaboration between governments, businesses and civil society	A long-term vision for data privacy	Develop new standards to promote interoperability and privacy-preserving data flows

PART ONE
TRACKING DOWN YOUR DATA

This section documents what happened when five volunteers attempted to track and retrieve their data. Demos researchers followed their attempts over many months to understand the challenges they faced.

We found a chaotic system that profits from our data, while doing little to empower users to exert their rights: data is collected and inferred about us, and used to make decisions in the dark about what sort of person we are, what sort of products and services we should be offered - from health insurance to mortgages. Through this investigation, as our volunteers uncovered how this economy actually operates with their information, they grew increasingly concerned about their data footprints. This was compounded rather than alleviated by the complexity and difficulty of the processes meant to be in place to empower them.

METHODOLOGY

This project is an exploratory investigation into how data sharing and data regulation practices are impacting citizens: looking into how individuals' data footprints are created, to what people experience when they want to exercise their data rights, and how they feel about how their data is being used.

We worked closely with five volunteers, across a range of demographics and with differing levels of online engagement, to investigate how companies using their data shows up in their own lives. We worked with a small group so that we could build a more in-depth and holistic view of how our participants engage with companies online, what this means for them individually, and how their data footprints meant they were being viewed online across the data system.

This also allowed the investigation to be guided by the participants: they were in control of what personal data they wanted to explore and share, and where they wanted to change what data companies were keeping on them.

As such, the amount and types of data we were able to collect and analyse varied across the volunteers. This report does not seek to present a large-scale or representative picture of the experiences of users generally online. Rather, it shines a light on how current commercial and regulatory practices are impacting on and being experienced by those who are meant to benefit from them: individuals, as consumers, data subjects, and citizens. It seeks to bring the perspectives of end users to the conversation about data protection which are too often missing.

The five volunteers included three women and two men. Their ages were 22, 25, 42, 52, and 66, and they lived across London, Cambridgeshire, Kent, and Edinburgh. They had varying levels of prior

familiarity with how personal data online is used.

Each of the volunteers signed a Participation Agreement before commencing their data discovery journey, outlining how this project would use their data and the control they retained over it. The data collection process was led by Rightly, and analysis by Demos. Rightly, Demos, Schillings and TVN worked with the volunteers throughout to support their participation in the project. Data collection involved participants providing the independent consumer data action service Rightly with both email data and data collected from various relevant companies (outlined in Table 1).

During an initial video interview, participants were asked questions about their digital lifestyle, as well as their attitudes and behaviours with regards to privacy online.

Each volunteer then used the Rightly Protect[9] service to identify, via their email inboxes, a list of companies who were contacting them and so held personal information on them.

The volunteers identified which companies they wished to delete their personal information from or not hear from again. Rightly then sent an email to each company on the individual's behalf to request that they delete any personal data being held. Any replies from companies were forwarded to Rightly and categorised as follows:

1. Automatic Response
2. Sent to IT dept/customer service department to deal with
3. Asks for confirmation that deletion is wanted
4. Advises consumer to delete their own account and data on the platform itself
5. Advises consumer to fill in online form or access privacy portal
6. Invokes data retention policy
7. Asks for further identification or details of relationship
8. No account or data found
9. Immediate or quick fulfilment to request for data deletion

Rightly also identified seven data brokers which they thought could potentially hold interesting data about the participants, these were: Direct Line Group (DLG); Crediva; GBG; Indicia; REaD Group; Equifax; and Experian Marketing Services.

Volunteers were asked to e-sign a Subject Access Request form which would identify and confirm that they had given Rightly permission to contact the data broker on their behalf. Rightly then emailed the Data Brokers and company responses were categorised as follows:

1. Sent but no response
2. Automatic response
3. Request for further identification
4. Request to visit their privacy portal
5. No data available
6. Data received

Finally, each of the volunteers were provided with instructions on how to request their data from Facebook and Amazon, which was provided to Rightly for review and assessment. Rightly also contacted two companies each for Volunteer A (Sainsbury's and the Guardian) and Volunteer B (British Airways and The Edinburgh Fringe), to find out what personal information was stored by them.

9 Rightly Protect. Available at: https://right.ly/rightly-protect/ [last accessed: 16/02/23]

Table 1 outlines the data that each volunteer contributed to the study. As can be seen from Table 1, a varying levels of data were provided across the participants, according to what each individual was comfortable with sharing. Some participants also joined the study later than others, meaning less data could be collected.

Rightly and TVN then conducted follow-up interviews with participants to discuss their experiences of the process of requesting the deletion of their data, and of what data was held about them.

Demos' data analysis divided into two categories, reflected in Sections A and B of this report. One stream focused on analysis of the process - how companies responded to Subject Access Requests and requests that personal information be deleted. The second stream focused on analysis of the data being held: the level of detail of data being shared, the extent to which and with whom data was being shared, and how volunteers felt about these outcomes. Volunteers participating in this report have reviewed and consented to the use of their data herein.

TABLE 1. VOLUNTEERS AND DATA TYPES COLLECTED FOR THE STUDY

NAME	DATA COLLECTED
Volunteer A	• Asked 174 companies to delete their information • Amazon advertiser and audience data • Experian data on household attributes, personal attributes and propensities • The types of personal information Equifax held about them (did not provide actual report) • Sainsburys customer report • The Guardian data (online comments)
Volunteer B	• Asked 188 companies to delete their information • Facebook advertiser data • Amazon advertiser and audience data • Experian Data Subject Access Request • Equifax Data Subject Access Request • Crediva Subject Access Report
Volunteer C	• Asked 115 companies to delete their information • Facebook advertiser data as well as requesting a record of all Facebook activity
Volunteer D	• Asked 72 companies to delete their information • Amazon advertiser and audience data • Facebook advertiser data

NAME	DATA COLLECTED
Volunteer E	• Asked 231 companies to delete their information

ONLINE IDENTITY

How online systems create identities for you that you are unaware of

Collecting users' data means adverts and services can be targeted and based on what is of interest to the consumer in question: personalised information is more relevant and interesting for the consumer, and more profitable for the companies involved.[10] Data collection and sales also provide an effective model for web monetisation, the process of turning web traffic into revenue. By collecting visitor's data, websites can stay free to use, unlike other forms of web monetisation like subscriptions and paywalls.[11] Web users who do not wish to be tracked like this can reject non-essential cookies, clear their cache or use privacy enhancing technologies. Web users who are less concerned about their privacy, or who actively want their data to be shared (to better personalise their internet services, for instance), can accept cookies.

However, over recent years it has become increasingly clear that this bargain isn't as simple and fair as it is presented to be. Online targeting can be used to send social media users into conspiracy and extremist groups.[12] People's online identities are gathered or accessed through cybersecurity attacks and weaponised against them in scams.[13] And the reality is that users often do not know exactly what data they are consenting to being shared, what could be done with it and where it could end up. This burden of invaded privacy is not shared equally across society: with a greater need for poorer individuals to share their data to access certain discounts, like through loyalty card schemes, or being unable to so easily afford paid-for privacy-preserving services.

Sometimes, the data that is shared, and the digital versions of ourselves constructed from this, might not even be recognisable to us.[14] Whether it's basic facts being wrong, to misjudged subjective qualities like our favourite newspapers, supposedly better-informed decisions that are made based on our data may be being made on shaky ground. When users cannot see what data is held about them and how these decisions are made, they are all left in the dark as to whether or not these decisions may be based on mistakes. And where these decisions are used to inform what services we might be offered or deemed eligible for, the ramifications can be significant.

The following section outlines the types of data that companies are keeping and selling about individuals, and how these practices contribute towards systems which create online profiles about people without them knowing. The data companies are keeping and selling on individuals to build these online identities can be broadly divided into two categories: data collected on people, and data that is inferred about people.

The data collected about you online can be both wide-ranging, and extremely granular and precise

The information that companies collect about individuals can be extremely granular in its level of

10 Data & Marketing Association. UK Data Privacy: What the consumer really thinks. 2022. Available at: https://dma.org.uk/uploads/misc/dma---uk-data-privacy-2022.pdf [last accessed 09/02/23]
11 Cummins, Ciaran and Victoria Baines. The Cost of Creation: What is a Fair and Desirable Future for Monetised Online Work and Volunteering. *Demos*. 2022. Available at: https://demos.co.uk/project/the-costs-of-creation-what-is-a-fair-and-desirable-future-for-monetised-online-work-and-volunteering/ [last accessed 09/02/23]
12 Matthews, Jeanna. Radicalisation pipelines: How targeted advertising on social media drives people to extremes. *The Conversation*. 2022. Available at: https://theconversation.com/radicalization-pipelines-how-targeted-advertising-on-social-media-drives-people-to-extremes-173568 [last accessed 09/02/23]
13 National Cyber Security Centre. Public urged to be aware of post-data breach scams. No date. Available at: www.ncsc.gov.uk/news/public-urged-to-be-aware-of-scams-post-data-breaches [last accessed 09/02/23]
14 Miller, Carl. Would you recognise yourself from your data? BBC News. Available at: www.bbc.co.uk/news/technology-48434175 [last accessed 09/02/23]

detail. Many of the data points held about individuals in this study were held at an individual level (rather than aggregate only), with a significant amount of very detailed personal information attached.

For instance, the Amazon data of volunteers included the messages account holders have sent to a vendor on its site, and the adverts clicked on its platform, detailing the business name and the number of clicks. One of our volunteers, Volunteer A, was also able to gain a Customer report from Sainsburys, which showed company retention of their residential neighbourhood type, the instore and online purchases they had made, as well as details about their loyalty cards and the campaigns and coupons they had been sent. Volunteer A was additionally sent detailed information from the Guardian online about the comments they had posted, their IP, the date, number of replies and country code.

Data of a very high, fine granularity is also collected about individuals by data brokers such as Equifax, Experian, Crediva and Direct Line. Through our volunteers' access requests, it was revealed that the data companies like these hold can include:

- Information such as name, address, date of birth, email, contact number, gender, occupation and vehicle
- Electoral roll history
- Financial repayment history
- Any credit searches or notices of correction on your credit report
- Current and past addresses you are linked to, including 'gone away' information (where someone no longer lives at their provided address)

There are clear and necessary business reasons to collect and store this data, for the business to provide a service that also benefits the user, for credit reporting and affordability checks, or identity verification and fraud prevention.

However, the fact that this level of data is being retained and that some of it is being shared for marketing purposes may not be obvious to consumers: one of our volunteers stated they "hadn't realised that when I accepted terms and conditions, that meant the company I was saying that to would then sell my information on".

What is likely to be even less obvious to consumers is that this kind of information, while useful to collect, can also be used to identify information about them that they may not wish to be shared. Even apart from more sensitive information about people's financial histories, less clearly sensitive information can have sensitive implications. For instance, collecting information on every item bought from a store over many years could potentially be used not only to infer information about what sort of products they may wish to buy in future, but more sensitive demographic information about their financial situation, their household, their lifestyle and even their health. This may well be a tradeoff many people are happy to make: but consumers should be able to assess the risks and benefits of these practices to themselves and make fully informed decisions.

Your data footprint includes wide-ranging assumptions about your characteristics, identity and how you are likely to act in the future: information which is sold on to enable more effective marketing

The data held by some companies acts differently to how 'personal data' is often conceptualised. Rather than definite information - links you clicked, messages you sent, food you bought - companies, like credit ratings companies, can hold 'propensities'. Experian describes propensities as "models which we build from market research data and which indicate how likely it is that an individual exhibits certain characteristics or behaviours".[15] These propensities can then be sold to other companies to deduce the most effective strategies when targeting particular groups of customers.

15 From volunteers' Experian Data Subject Access Request document.

Propensities represent the heart of the data economy: dataify as much behaviour as possible, situate it within large datasets to create a shadow digital identity that can be used to craft a digital environment optimised for advertising.

The most detailed data assumptions in this study come from the data broker Experian's Data Subject Access Request reports. These were acquired by two of our volunteers. These are models calculated by Experian to make inferences about the personal or household attributes of an individual. Personal attributes might include variables such as who is the head of the household, marital status and personal affluence level. Household attributes might include variables such as estimated affluence level, council tax band, family life stage or number of adults in the household. Together, these modelled assumptions constitute a detailed picture of an individual's private life.

Grouping the propensities shared by Experian on our volunteers paints a picture of what companies want to know about their target customers. Experian supplies "marketers, product developers and customer acquisition teams"[16] estimations about financial behaviours (the kinds of investments someone might hold, sources of debt, use of price comparison sites, amount of money donated to charity) to more mundane (places you might visit in your spare time, sources of news, what you use different digital devices for, which supermarket you visit and how you like to buy your groceries).[17]

Data was also gathered from Facebook on our volunteers, which was largely about advertisers and consists mainly of business names which Facebook infers an individual might be interested in, in contrast to the specific personal details as was observed with the data collected about individuals.

Facebook advertiser data was collected by three out of our five volunteers to various degrees. Both Volunteer C and Volunteer B were also able to access information on their 'Ads interests', data which shows what businesses or organisations Facebook thinks an individual is interested in. Volunteer B found 298 companies Facebook had associated with their account, whilst Volunteer C found 246. Volunteer C was the only volunteer to also provide their audience based advertisers, companies targeting them as they shared characteristics with others who buy/interact with their products and services, finding 51 companies associated with their account in this way. All of these different data sources help in contributing towards an online identity about our volunteers that Facebook is constructing behind the scenes.

Three of our volunteers were also able to provide us with data about the types of inferences Amazon makes about its users. Perhaps the most interesting data from this website is the 'Amazon audiences in which you are included' data sets. From this data set, we can see that Amazon account holders are sorted into wider thematic 'audience' groups on the website according to what Amazon thinks they might be interested in, from Arts and Crafts to Pet Supplies and Western movies. Three of our volunteers were able to retrieve this information, with Volunteer A finding they had been sorted into 31 audiences, Volunteer B 29 and Volunteer D 43. Volunteer B and Volunteer D also found that they had been added into audiences through data from 3rd parties (2 audiences and 1 audience respectively). All three of these volunteers were also provided with data on 'Advertisers who bought audiences in which you are included' in the form of a list of companies.

There can be hundreds or even thousands of different companies which are using your data to target advertising

All three of the volunteers were able to source information on 'Advertisers using your activity or information', which consists of a list of companies and businesses that have entered information they gather 'off platform'. According to Facebook, this pertains to information that is collected when businesses and organisations share information that they have gained through a Facebook Login or Facebook Pixel; often through an individual logging in to an app with the individual's account, visiting a website, searching for an item or purchasing an item which in turn influences what Facebook

16 Lindsay, Mark. How to understand engage your customers through data. *Experian*. 2018. Available at: www.experian.co.uk/blogs/latest-thinking/marketing-solutions/how-to-understand-and-engage-your-customers-through-data/ [last accessed 09/02/23]
17 For full list of propensities see: Experian. Modelled marketing data. 2022. Available at: www.experian.co.uk/content/dam/marketing/uki/uk/en/pdf/modelled-marketing-data.pdf [last accessed 09/02/23]

assumes the kinds of adverts an individual would like to be targeted with.[18] Facebook admits that not all the data they hold about a user is shared when this data is downloaded, claiming that due to "technical and accuracy reasons, we don't show all the activity we've received. This includes things like information we've received when you're not logged into Facebook, or when we can't confirm that you've previously used Facebook on that device. We also don't show details like the item you've added to your shopping cart".[19]

Volunteer C found that 2,242 companies were using their 'off-Facebook' interactions to target their advertising, whilst this number was 316 for Volunteer D, and 94 for Volunteer B.

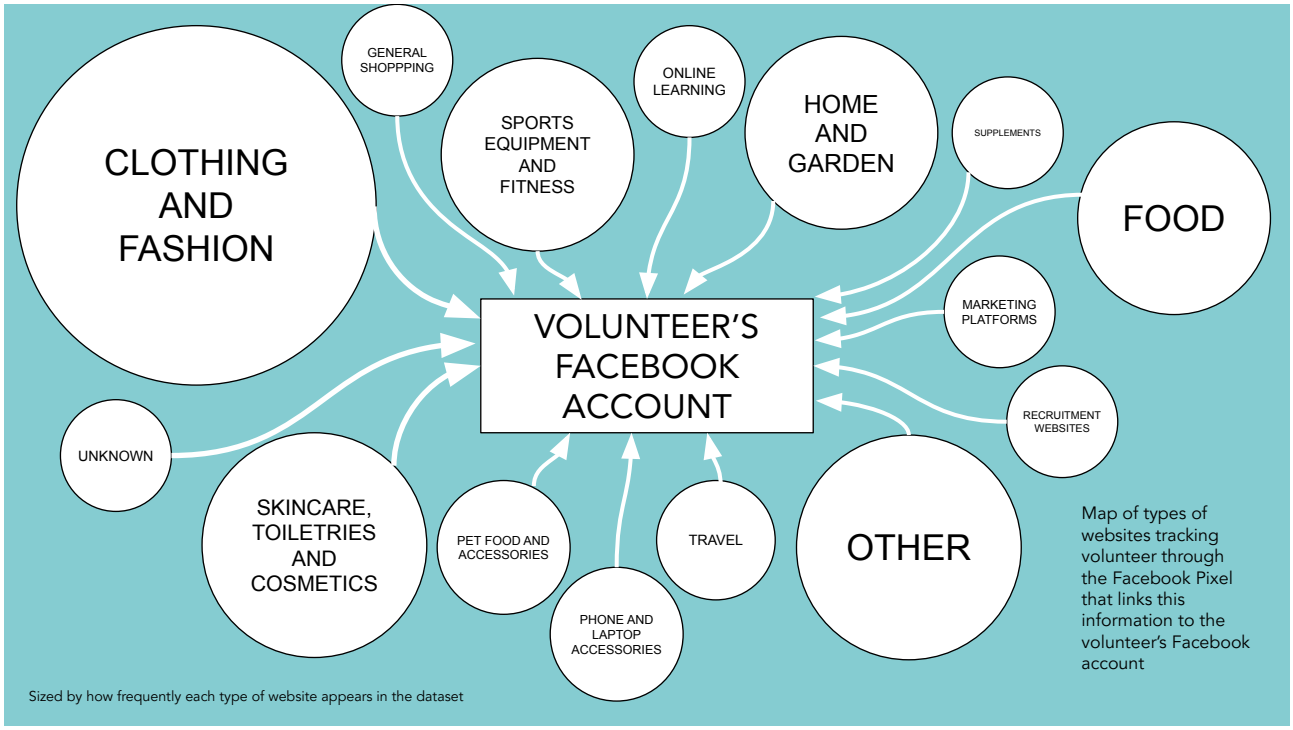
Two of our volunteers were also able to receive information on how Facebook uses 'Apps and Websites' to access information about an individual to inform advertisers. Volunteer C found that 20 live apps were using their information, and 68 expired apps had accessed their data in the past. Volunteer B also discovered that 6 live apps were accessing their information and 31 expired apps had in the past.

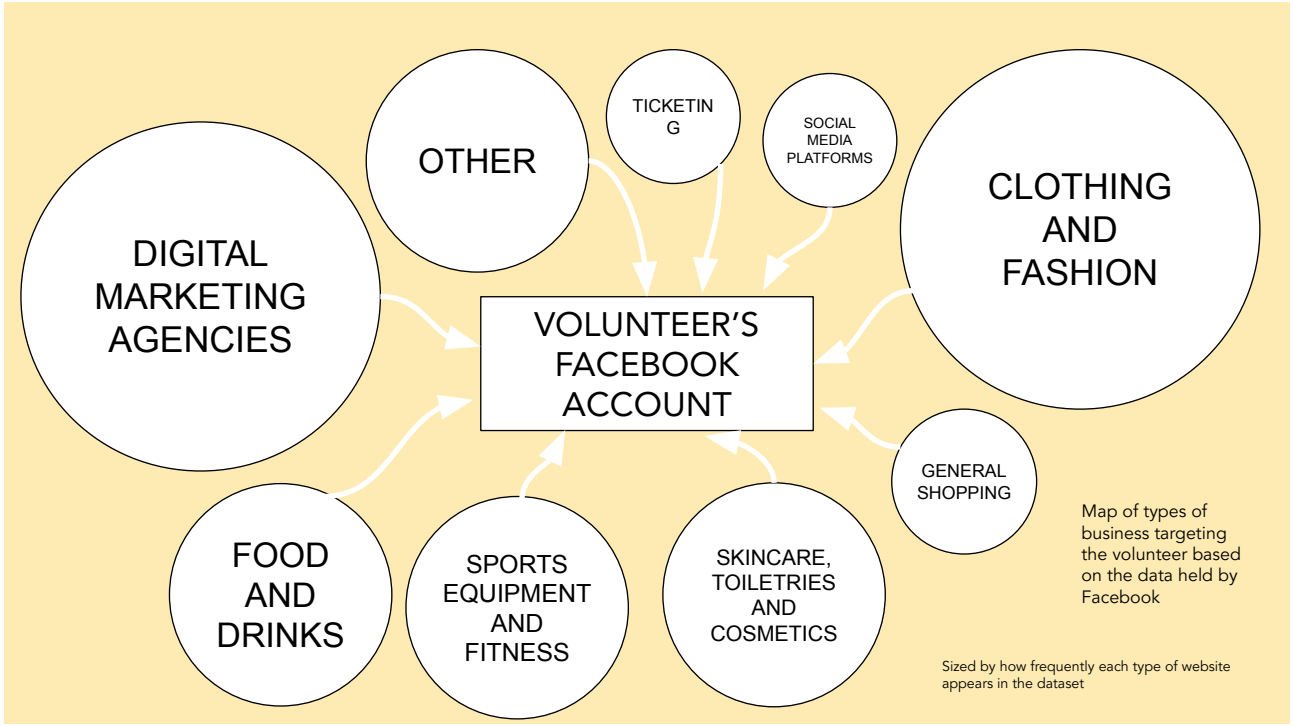
Using one website or application is just one point in a chain of companies collecting and buying your data

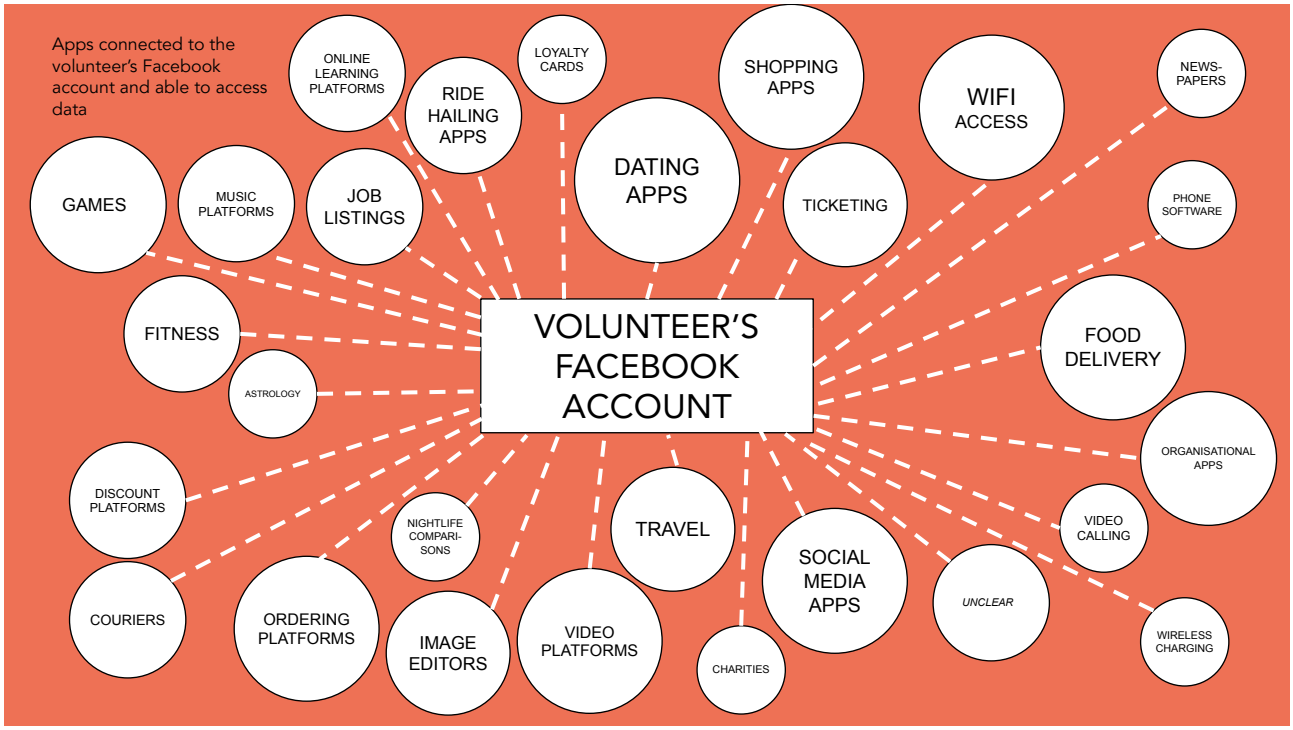
- Taking one volunteer's Facebook account we mapped the companies accessing their individual's data. There were three ways that companies became linked to their account:
- Through the Facebook Pixel, a line of code on websites that allows visitors to be linked to their Facebook accounts.[20] (2,242 companies)
- Through targeting advertising audience groups[21] containing the volunteer. (51 companies)
- Apps where the volunteer logged in via their Facebook account. (20 live apps, 68 expired apps)

Taking a random sample of 100 of the 2,242 companies that had targeted Volunteer C via the Facebook Pixel and all of those that had targeted them based on advertising audience groups or could access their account through their login information, each company was checked and classed based on their product or service. Using these groups, the following maps were made demonstrating the kinds of companies that just one Facebook account can get connected to:

18 Facebook. Review your Off-Facebook activity. No date. Available at: www.facebook.com/help/2207256696182627 [last accessed 09/02/23]
19 Ibid.
20 Meta Business Help Centre. About Meta Pixel. Meta. No date. Available at: www.facebook.com/business/help/742478679120153?id=1205376682832142 [last accessed 09/02/23]
21 That is, groups of likely similar people as determined by Facebook


GENERAL SHOPPPING
SPORTS EQUIPMENT AND FITNESS
ONLINE LEARNING
HOME AND GARDEN
SUPPLEMENTS
CLOTHING AND FASHION
FOOD
MARKETING PLATFORMS
VOLUNTEER'S FACEBOOK ACCOUNT
RECRUITMENT WEBSITES
UNKNOWN
SKINCARE, TOILETRIES AND COSMETICS
PET FOOD AND ACCESSORIES
TRAVEL
OTHER
PHONE AND LAPTOP ACCESSORIES
Sized by how frequently each type of website appears in the dataset
Map of types of websites tracking volunteer through the Facebook Pixel that links this information to the volunteer's Facebook account


OTHER
TICKETIN G
SOCIAL MEDIA PLATFORMS
CLOTHING AND FASHION
DIGITAL MARKETING AGENCIES
VOLUNTEER'S FACEBOOK ACCOUNT
GENERAL SHOPPING
FOOD AND DRINKS
SPORTS EQUIPMENT AND FITNESS
SKINCARE, TOILETRIES AND COSMETICS
Map of types of business targeting the volunteer based on the data held by Facebook
Sized by how frequently each type of website appears in the dataset



Working through this data exposed some common themes: clothing, sustainability, fitness and dating apps. Spending time with this data emphasised not just how far Volunteer C's data is spread, but also how seemingly intimately connected with their interests the data are.

There were also ambiguous companies involved. 11 of 51 companies (20%) targeting Volunteer C through advertising groups were marketing agencies, meaning it was ambiguous whether their data was being shared from that point and to whom, as that would only be determined by contacting those companies to enquire about the volunteer's data. Similarly, 7 apps they had logged into with their Facebook account were means to access public wifi. These wifi apps also sell themselves to businesses as ways to collect data on the customers in their stores.[22] Again, it becomes ambiguous which companies were accessing data through these companies.

Together, these diagrams begin to reveal the nature of data flows. Users are targeted with advertisements and products, data about their interactions with these are then collected and sold on, this information is assessed to make more decisions about them, which in turn shape the environment in which users find themselves. The decisions that users make - which apps to log into via their social media accounts, which adverts to click on or which ones to scroll past - are one tiny piece in a chain that they do not have the ability to fully access.

This goes far beyond what data people are expecting is held on them

On seeing their data, many volunteers were shocked and surprised to find out both what data is held about them and how this data is sold.

It was clear from these reactions that the current norm of accepting terms and conditions is inadequate. Alongside the volunteer who had not realised that accepting terms and conditions meant agreeing to have your data sold on, another was "*intrigued about how we are all constantly accepting cookies for our information to be tracked, and a lot of the time we don't read the terms & conditions, so we don't know what we're agreeing to and how our information is being tracked and collected and being made available to businesses that I don't really know*". There is an immense amount of opacity in data collection and sales resulting in an extreme information asymmetry that is disempowering for internet users.

22 See for example: Captini. Available at: https://captini.com/social-wifi [last accessed 09/02/23]

Sometimes platforms also fall foul of this information asymmetry as a volunteer described *"one of the biggest problems right now is social media companies gathering enormous amounts of data on people, selling it off to data brokers and even they don't know where it ends up"*. Even after trying to track down as much personal data that is held about you as possible, there is a limit as to how much you can know as even companies themselves can lose the trail: leaving users unable to know what is happening with their data.[23]

Discovering this information asymmetry left one participant feeling *"scared"* and *"concerned"*, because *"there's information about me out there, that I don't know what people are doing with"*. The current data economy leaves people unable to control their identities, and construct digital identities that the volunteers didn't even recognise: *"What I'm very horrified by is the fact they think my main daily newspaper is the Daily Mail, which is totally wrong"*.

Not being in control of who holds your personal data can leave people vulnerable if bad actors are able to gain access to the data (for instance, through hacking). One volunteer had experienced the risks of personal data being shared publicly about them. They experienced someone "*[writing] an article in which [this person] listed [the volunteer's] family members, their places of work, [their] home address, lots of sort of very personal and identifying information which is very dangerous to have in the hands of those kind of people"*. They also stressed that these risks are more acute for those at risk of being stalked or those who are victims of domestic abuse, where abusers *"have been able to go to these people finding websites and finding information about their partners they want to abuse or their stalking victim"*. A recent high-profile example of this was the harassment of LGBTQ+ people by extremist websites, which included sharing personal details, including those obtained through hacking companies to access private data.[24]

Having seen the data held about them, the volunteers describe a desire *"to be more wary about what I sign up to"*. On realising the lack of care some companies may take in containing their data, for a participant that wariness is *"not necessarily about that I don't trust them as a brand to not misuse my data it's the fact that I don't know who they're selling it to, and who that data broker is selling it on to"*. As the data economy is currently constructed, citizens are left in the dark about their personal data.

THE BIG LIE

How processes meant to empower users to be in control of their data do the opposite

The promise of data protection legislation has been great: a new era of empowerment, in which users hold significant rights over their personal data: the right to request their personal data from a company that holds it, the right to revoke permission for a company to use it for certain purposes, the right to request it be deleted. However, for many people their main interaction with GDPR is through the now-infamous 'cookie banners', which are an annoyance at best, but at worst actively seek to dissuade you from changing your data permissions, through nudges to incentivise you to agree to the most permissive settings.

This project sought to investigate what the experience of requesting personal data deletion from companies was like for individuals, in particular how able they were to exercise their data rights, including:

The Right of Access: 'You have the right to ask an organisation whether or not they are using or storing your personal information. You can also ask them for copies of your personal information, verbally or in writing.' [25]

The Right to get your Data Deleted: 'The right to get your data deleted is also known as the 'right to erasure'. You can ask an organisation that holds data about you to delete that data. In some

23 Bhuiyan, Johana. Where does your info go? US lawsuit gives peek into shadowy world of data brokers. *The Guardian*. 2022. Available at: www.theguardian.com/technology/2022/mar/23/data-brokers-lawsuit-security-transparency [last accessed 09/02/23]
24 Collins, Ben and Kat Tenbarge. Anti-trans stalkers at Kiwi Farms are chasing one victim around the world. Their list of targets is growing. *NBC News*. 2022. Available at: www.nbcnews.com/tech/internet/cloudflare-kiwi-farms-keffals-anti-trans-rcna44834 last accessed 09/02/23]
25 ICO. Your right of access. No date. Available at: https://ico.org.uk/your-data-matters/your-right-to-get-copies-of-your-data/ [last accessed 09/02/23]

circumstances, they must then do so. You may sometimes hear this called the 'right to be forgotten'.'[26]

Trying to take control of your data is complicated, time-consuming, and no guarantee of success

Volunteers were asked to go back as far as possible through their email inbox using Rightly Protect to identify companies that are likely to hold data on the volunteer. This produces a list of companies that the volunteers could then review and decide which companies they would like to ask to delete their data. Rightly Protect then sends an email to each of the identified companies, in the individual's name, to request that they delete any personal data that they hold. As response emails came to the volunteers, they forwarded them to Rightly who compiled and categorised the kinds of replies the volunteers received. These replies included automatic acknowledgement responses, confirmation of immediate data deletion, referral to different departments, or an explanation that it is necessary to retain the data.

This process stems from the UK GDPR's right to erasure, or 'right to be forgotten' as it is more commonly termed.[27] Organisations have one month to respond to a request once it is made, whether that is in writing or verbally. There are reasons an organisation can legally maintain the data after a erasure request has been made, for example if they are legally required to hold that data, and individuals making the request must be informed if this is the case. If companies can only hold or use that personal data based on consent and that consent is withdrawn, the data must be deleted.

The right to erase data is a key way that internet users can exert control over their data in a system that is otherwise structured to stop them doing so. Without it, and without the proper enforcement of it, the notion of 'consenting' to data collection becomes flimsy.

However, the picture painted by the requests to delete data sent by volunteers suggests that the reality of the extent to which users are able to exert the right to have their data erased is a mixed landscape. Individuals can expect any range of responses from companies, some who will comply immediately with data protection laws, and others who leave users without a clear answer. The route to get there is also often laden with difficult-to-navigate barriers. There is little consistency, meaning that consumers are unable to set their expectations about what a company will do with their data at the point at which they have to decide whether to consent to share that data initially.

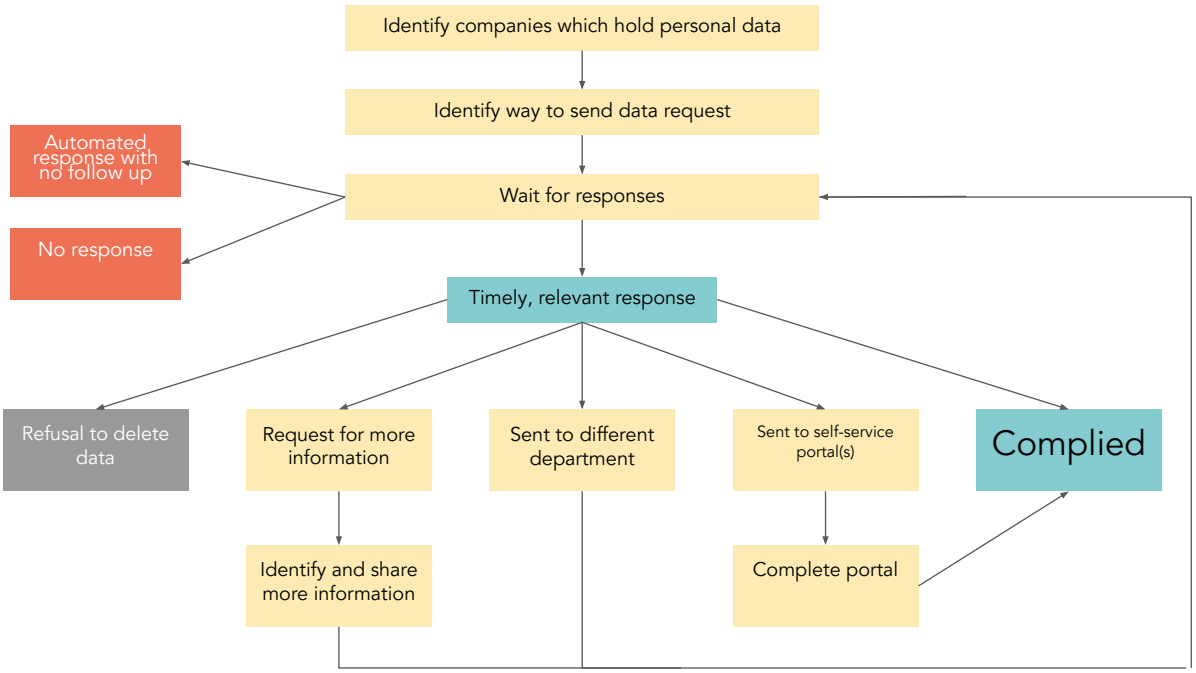
The process: increasingly complex and requiring a great deal from the user

To begin to understand where your data could be and to start deleting it requires citizens to be dedicated, time-rich and digitally literate. Many people will face serious barriers in undertaking these processes, especially if they work long hours, have multiple jobs or caring responsibilities, or face difficulties or need support in using digital services. Taking seriously the impossibility of tracing and deleting personal data challenges what it means to 'consent' to data collection and points to deep flaws in data sharing systems as they are constructed.

A schematic of the process undertaken by our volunteers in partnership with Rightly is below:

26 ICO. Your right to get your data deleted. No date. Available at: https://ico.org.uk/your-data-matters/your-right-to-get-your-data-deleted/ [last accessed 09/02/23]

27 ICO. Right to erasure. No date. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ib7 [last accessed 09/02/23]



Even using a service such as Rightly Protect, which enables a great deal of this to be automated, the process is time-consuming. As companies respond effort must be taken to track who has replied, who has not, who is adding extra friction to the process by requesting further information to be able to delete the data.

"Thinking back on the process of some of them it was really long-winded. One of them you had to register online, then wait for a password to come in the post, and then you go in and then you request your stuff. If I was doing this for real … because I was genuinely concerned, it's a job in and of itself, you have to manage each one, see when they respond."

Our volunteers described elements of the process as deeply frustrating: one found "self-service privacy portals very, very annoying"[28] and attempting to interact with one major supermarket "just infuriating". Another "didn't think there would be that many responses, I didn't think also that there would also be… not work, but that I'd have to be logging back into my emails to check whether [Rightly] had wanted more information or wanted things forwarded on".

And bearing in mind this process only comes into contact with the data that can be revealed by a participant's email address, there will be wealths of personal data gathered through other websites and applications that are not present in their volunteer's inbox left untouched by this process.

Where details of the personal data was requested through Subject Access Requests rather than data deletion requests, further effort and time is demanded on a person wanting to understand what has happened to information about them. Lists returned from Facebook, for example, are of frequently obscure companies that require further analysis to fully understand, only for it to become clear that some of those companies are likely to have sold your data onto further companies that would require yet more effort to trace. Other data returned from Facebook included lists of thousands of companies that had tracked a participant's movements across the internet via the Facebook Pixel.

28 All quotes in this section from documentary footage.

Data requests were often complied with: but not clearly or consistently

FIGURE 1
RESPONSES TO DATA DELETION REQUEST

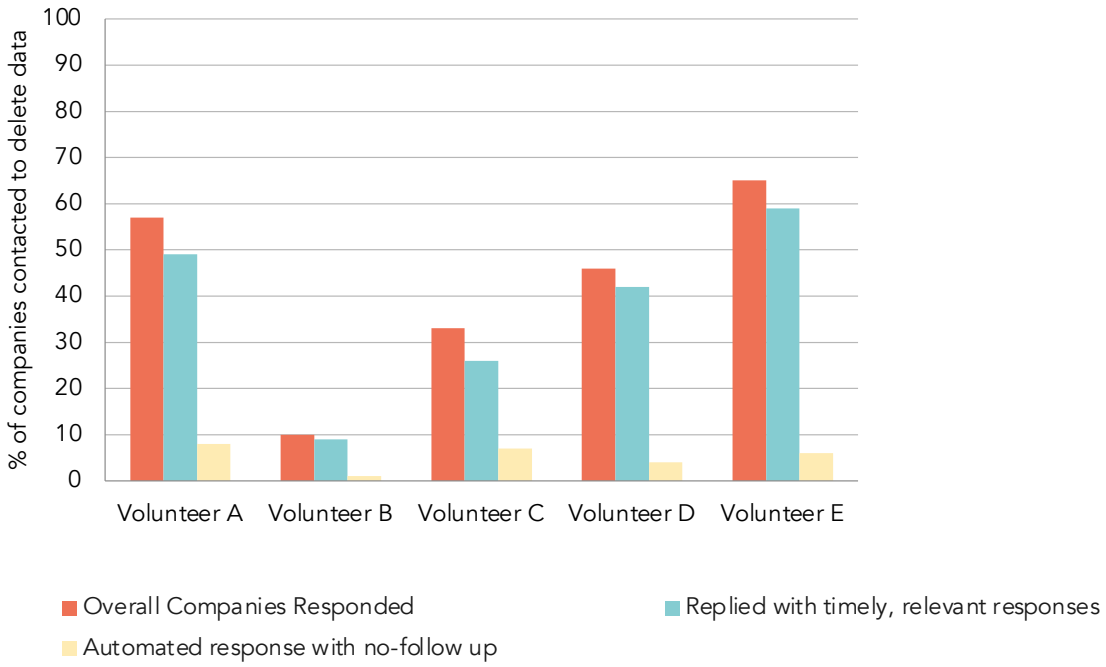
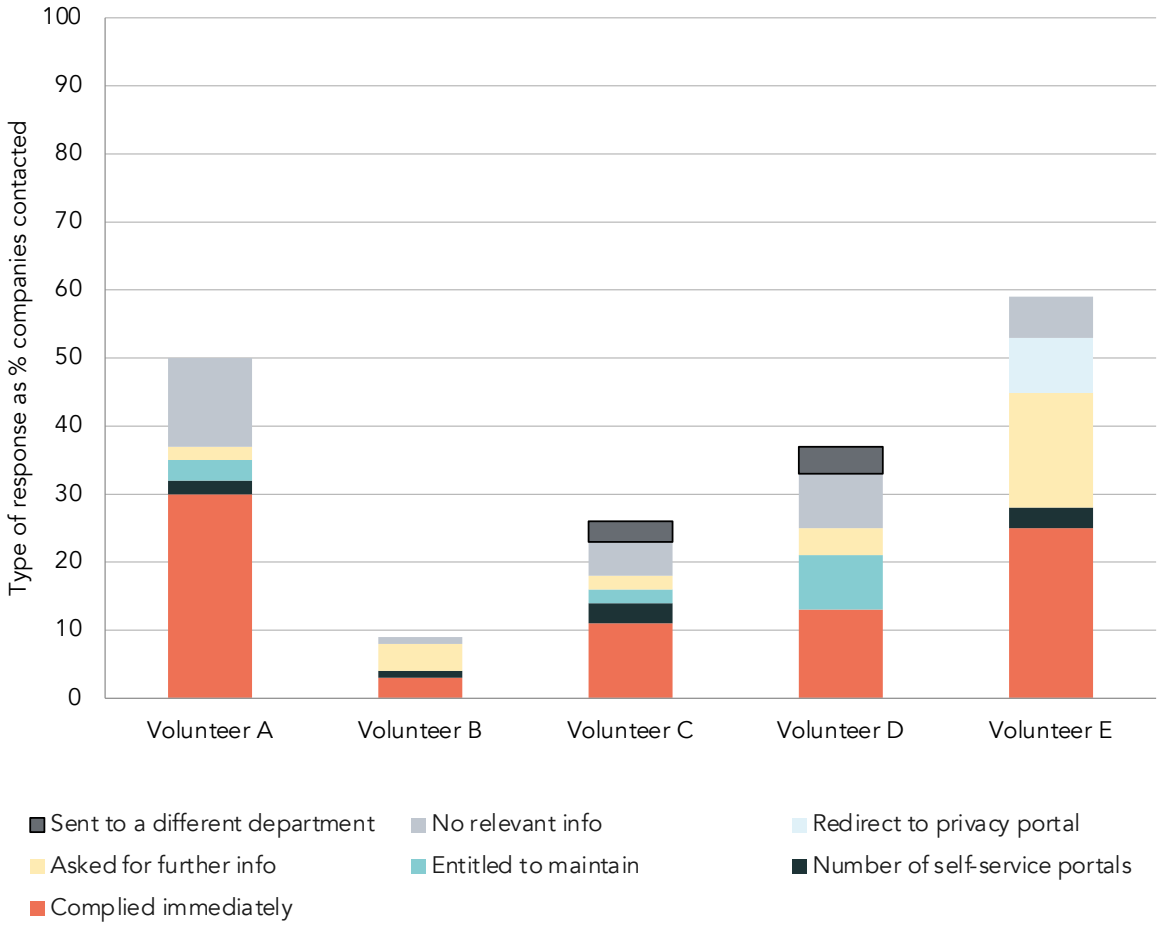


FIGURE 2
BREAKDOWN OF TIMELY, RELEVANT RESPONSES



From data provided by Rightly. Full data in the appendix.

There were positive outcomes from engaging in these processes: where the processes set up through GDPR were able to be used by volunteers to successfully control and manage their data.

Where companies did respond to the volunteer's request to delete their data, most of those responses were relevant and timely. Three of the participants received these kinds of responses from the companies contacted. Most of those timely responses were companies immediately complying and deleting the data. Equally important to note are the number of companies that do not hold relevant data, suggesting that data is being deleted as required. Alongside the data deletion requests, Facebook, Amazon, Sainsbury's, the Guardian and the seven data brokers contacted did also return the data that was requested. There is clear evidence of good practice and that in some instances individuals are able to exert a level of control over their data.

But these positive instances are far from the full picture. Most companies did not comply immediately, many sent automatic replies that weren't ever followed up on, and volunteers encountered unexpected barriers to referrals to different departments or privacy portals. It is unclear from this whether or not the participant's data was deleted, or even if those companies did hold the data. The uncertainty in what is happening with this data demonstrates that the reality of data protection is one of frustration and confusion. Even where individual companies demonstrate good practice, for an individual to begin to take control of their whole footprint across the data ecosystem is a monumental task.

Often companies are not able to delete user data even upon request

The right to have your data deleted is not absolute - it is qualified either by interaction with other legal requirements that companies have around data retention, or due to the terms set out in the companies' own data and privacy policy: policies which are often hard to find and hard to understand, and can mean that companies are keeping personal data for many years.

Companies may also not refuse outright to delete data, but refer users to contact a different department, ask people to provide more personal information in order to enable them to identify the data to be deleted, or say they have no data to delete. Some of this will be absolutely necessary for the company to be able to manage data compliance requests effectively - but it speaks to a system that the pay-off of this compliance for the end user is not clarity or control.

The reasons that companies gave our volunteers for not deleting their data included:

- That they were entitled or obliged to retain financial information about transactions due to HMRC requirements
- That they needed to retain the data for a period of years in order to facilitate retrospective analysis, or to ensure that insurance claims are handled correctly after the expiration of a policy
- That the data was being held legitimately in line with their retention policies
- That they were required by law to retain the information

The information that companies requested before deleting personal data included:

- More identification
- Exact details, such as bookings, account information, addresses orders were sent to, websites the user had interacted with, health practices which held their information

Quotes from companies' responses included:

"As part of our review we have determined that this data is currently being held legitimately in line with our retention policy of 12 months. Whilst we are unable to uphold this element of your request and delete your data at this time, we can confirm that this data will be deleted from our systems on or around [date]."

"Be aware that we are unable to delete your data because you have placed an order with us on [date]. We are compelled by HMRC to hold customers personal information surrounding said order for 6 + years."

By the time all of the responses had been received, one of our volunteers was "surprised that only 50% of companies responded in any way" and was left confused that "some companies say that they didn't have information on me, but I know we had contact or bought something from them so I don't understand that".

The systems and processes can work - but there are huge limitations for individuals trying to exercise their data rights

Parts of data protection processes are working. Our volunteers' experience, although mixed, does demonstrate there are systems in place that people can use and ensure that their data is deleted where that is possible. Companies hold increasingly large and complex sets of data, and it should be expected that a number of companies will be slow or need additional systems to be able to access the information they hold on an individual. For most users, the data-driven economy can mean better, more personalised and more efficient services and products. Users value this and many happily use these services.

However, these systems have significant limitations. The current processes are not ones that can be easily scaled for a user to manage and see their data holistically. Instead it requires intensive scouting of who has their data, who has sold what data onto whom, and the need to follow up with those companies if they truly wish to follow the trail of that data. It is a laborious process: the volunteers required whole research teams to support them to collect and make sense of their data. While the current situation is often difficult, confusing and fallible, it does work well for individual instances where a user wants to have their personal data deleted by one company. Even this system is better than having nothing at all.

But this is not a suitable system to work across a person's whole data ecosystem. At the moment data is generated as a means of tracking users across the internet, with no clear way for users to understand what that data is, see a record of where it has been shared, what is being used for and whether it is being stored in a secure way. Instead, there is a huge information asymmetry between users and the companies who hold their data, which takes the form of policy details, the legal requirements of data protection, accountability and access to recourse if companies do not respond to data deletion requests, and what users can do in the instance of hack or worsening cybersecurity situations at companies.

Despite being disadvantaged in terms of resources and ability to profit from the data in question, the current system is designed to put a huge burden on users to navigate through these barriers. This responsibility needs to be shifted to place a greater burden on companies to, for example, reduce the information asymmetries, and also onto governments and education to improve data literacy amongst the public so there is a greater understanding of how and why personal data is used, and what rights an individual has.

Finally, it is important to note that while consumer choice should be respected and many users would continue to trade their data for the kinds of services they can receive online, this choice is not unconstrained for some users. Sharing data in exchange for free services is a key principle of the data economy, and to access services and products that do not share users data often costs money. Privacy is, in this way, also a matter of digital exclusion where the consequences of obscured data sharing are a greater burden on those who cannot afford to opt out.

The next part of this paper sets out what the policy responses should be to the experiences we outline above.

PART TWO
FUTURE POLICY SHAPING

In our research, we found a chaotic system that profits from our data, while doing little to empower users to exert their rights: data is collected and inferred about us, and used to make decisions in the dark about what sort of person we are, what sort of products and services we should be offered - from health insurance to mortgages. Through this investigation, as our volunteers uncovered how this economy actually operates with their information, there was deep concern about their data footprints. This was compounded rather than alleviated by the complexity and difficulty of the processes meant to be in place to empower them.

But this is not an inevitability of a digital future. Our research sought to identify and explore the problem: the status quo of the data economy, where citizens are too often left powerless to have control over their data.

Here we set out a path forward, exploring the innovative ways that are already emerging of defending privacy, and identifying what different stakeholder groups can do in the short and longer term to protect privacy and change our relationship with our data for the better.

As well as building on our research, we summarise and develop the contributions made and discussions held through three stakeholder roundtables in November and December 2022. Participants included academics, lawyers, technologists, people working in industry and civil society. The roundtables, held under Chatham House rules, focused on diagnosing the problems and what potential solutions already look like, or could look like in the future, across multiple stakeholder groups.

Participants at our roundtables who were happy to be named in this report, as well as the Schillings and Demos teams, included:

Jonathan Baggaley

Mark Bembridge

June Brawner

Elinor Carmi

Prerak Mehta

Jon Nash

Will Nicholson

Jen Persson

James Walker

The roundtables dealt with three key questions:

1. How far can the privacy challenges arising from the rapid development of new technologies be addressed by the use of better or different technologies?
2. In a world where data harvesting is seen to give companies a competitive edge, what are the commercial advantages for protecting privacy?
3. How can we keep children, a particularly vulnerable group online, safe online without relying on intrusive levels of surveillance?

DIGITAL ACTORS

Who can make change happen?

It is no overstatement to say that the rapid growth in data-driven technologies and techniques has transformed our society. As a consequence, data systems are a complex network of stakeholders with varying degrees of ability to effect change.

Our discussions covered the role that individuals, as users, citizens and consumers; civil society, academics and researchers, governments and regulators, and business and industry can all play in changing the outlook for the data economy.

Below we present an overview of the relative roles, powers and limitations of these stakeholders that came out of our policy roundtable discussions:

STAKEHOLDER	POWER TO INFLUENCE DATA ECONOMY	LIMITATIONS TO THEIR POWER
Individuals	Strength of the data economy is driven by the fact that people value the services it enables: from free use of social media to more accurately tailored and relevant products Collectively, growing concern and advocacy for privacy can build pressures on businesses, governments and researchers to make privacy-positive choices Users have some powers currently: can consent or not to cookie collection, can turn personalisation off for some services, can request companies delete data	Collective public advocacy for change is difficult in a monopolised tech market where certain data practices dominate Accessing redress if our data is misused or being able to compel compliance are out of reach for most people: and particularly children Time, knowledge and the resources required to make more privacy-preserving choices not available equally to everyone: overcoming friction in the system is difficult

STAKEHOLDER	POWER TO INFLUENCE DATA ECONOMY	LIMITATIONS TO THEIR POWER
Governments and international institutions	Legislation sets the boundaries as to what may or may not be done with personal data International cooperation can support wider and more powerful standards regime Governments can invest in initiatives such as development of privacy-preserving technologies and citizen digital literacy	Have to balance benefit of regulation with potential costs around innovation and growth Efficacy of regulation relies on efficacy of enforcement regime
Regulators	Set standards that companies must meet Able to impose material (and reputational) costs on companies for non-compliance	Resources to pursue enforcement limited Companies may 'price in' fines to their everyday business
Civil Society and academia	Develop methods and models for best practice in ethical data-sharing Support digital and privacy literacy amongst citizens Advocate for greater privacy protection	Limited resources Lack of transparency from private companies about how data is being used or access to data
Business	Innovate and invest to develop new models, technologies and data practices, employing privacy-by-design principles Empower customers to understand and control how their data is used Demonstrate the consumer and business benefits of a privacy-first approach	Being competitive in a market dominated by tech giants who rely on data-driven business models

CURRENT POLICY

The status quo

A widespread understanding of personal data and privacy rests on the core question: do we have control of who can access or use our information, or do we not?[29]

This gives rise to a view of the challenge as one where each individual owns and should be in control of a certain bundle of private personal data, which contains valuable information about them. Data-driven business models mean private companies seeking to extract that data, and using the information to further their business, such as through targeted advertising. But once extracted, individuals then have little to no control over, or even knowledge of, how their data will be used.

This sets up an arms race between data extract-ors and data extract-ees, which the individual will likely lose, having far fewer resources at their disposal. The role of governments and regulators becomes to try to mediate - requiring that users be given more choice about whether to hand over their information or not. But this 'pull up the data drawbridge' approach: (if you want to protect your personal data, do not consent to sharing it under any circumstances) also can have negative effects for society more widely. During the Covid-19 pandemic, this came to the fore: countries across the world struggled with how to collect certain kinds of data about individuals to protect public health, and the resulting infrastructures were often not trusted, not effective and/or not privacy-preserving.

When data is shared within the current system, the structure of incentives mean the following problems persist for businesses, researchers, and individuals, highlighted in our roundtables.

STAKEHOLDER GROUP	PROBLEMS WITH STATUS QUO
Individuals	Current systems meant to empower users, such as cookie banners, or Subject Access Requests, are inconvenient and opaque: and focus at consent for data use at the point of collection, rather than an ongoing process Personal data collection can put users at risk of fraud or doxxing, if data leaks or is misused Users may face unfair restrictions where their access to services is based on an incomplete data profile (such as with respect to credit scores, mortgages, insurance)
Businesses	The quantity of user data available to companies can be vast, the quality is often low, as the data is the incomplete sum of various digital traces, which may be largely inaccurate, or irrelevant for many purposes. Mass collecting data entails many responsibilities for companies aiming to comply with policies on responsible data storage and allowed uses, a burden which grows heavier under stricter regulation. Failing to comply has seen huge fines levied against companies in breach of regulation, most notably with Meta being fined a total of €390m for forcing users to opt-in to having their data used for targeted advertising.[30] Small companies may be more affected by the costs of compliance and unable to weather fines.

29 See our previous research: Judson, Ellen. A Room of One's Own: A guide to private spaces online. *Demos*. 2020. Available at: https://demos.co.uk/project/a-room-of-ones-own-a-guide-to-private-spaces-online/ [last accessed 16/02/23]

30 Milmo, Dan. Meta dealt blow by EU ruling that could result in data use 'opt-in'. *The Guardian*. 2023. Available at: https://www.theguardian.com/technology/2023/jan/04/meta-dealt-blow-eu-ruling-data-opt-in-facebook-instagram-ads [last accessed 16/02/23]

STAKEHOLDER GROUP	PROBLEMS WITH STATUS QUO
Researchers	Researchers can face prohibitive costs or significant barriers to access data

THE WAYS FORWARD

Round table recommendations

There are clear ways that current practices are not living up to the standards they have set themselves, or consumer expectations. Our roundtable discussions highlighted the importance of identifying and pursuing changes which can be implemented in the relatively short term and within existing frameworks to better protect and promote privacy, such as the following:

Businesses have the power to adopt new innovations in privacy protection, including:

- **Adopting new ad-tech solutions that drastically reduce the amount of tracking and data collection required**[31]. For example, by using zero-party data collection where adverts are targeted based on information collected directly from the relevant user such as through surveys or parts of your website interacted with, rather than based on information gathered and sold through other trackers. These techniques drastically reduce the amount of data collected and held on each individual user, while retaining personalised advertising that many businesses require to operate effectively online and many consumers want.

- **Incorporating privacy-by-design**. Businesses like Apple and WhatsApp have demonstrated both the success of privacy as a selling point, and as a means to force change in competitors who do not have a focus on privacy. Looking to integrate ways to preserve privacy in the design of products and systems, such as through end-to-end encryption or adopting differential privacy[32] (where data is made noisier to hide the individual it is gathered from) protects consumers from the beginning. Brands should seek to make this known in their marketing both to build trust and push for a better business landscape overall.
- **Assessing where data is likely to be collected on children and developing safeguards to reduce the amount of data collected on children**. Companies should ensure compliance with the Age Appropriate Design Code,[33] which includes ensuring that data sharing controls are easily understood by children, do not nudge them to share data unnecessarily and only use profiling to share age appropriate content. Focusing on making services age-appropriate services can also help reduce the need for age-verifying users before they are able to access that service.
- **Develop more easily accessible terms of service**, which explain how users' data is being used, for what purposes, for how long. This should be based on evidence and user engagement to establish how users can best understand what they are being asked to consent to, and consent proactively sought to continue using data periodically.

Governments and regulators can also play a role in improving online privacy, through interventions such as:

- **Stronger, clearer and more easily accessible enforcement mechanisms for privacy violations, including enforcement of the UK GDPR**. Inconsistent enforcement of existing regulation, a lack of clarity about how enforcement operates, and poor practices across industry, means citizens don't

31 Salesforce. What is Zero-Party Data? No date. Available at: https://www.salesforce.com/resources/articles/what-is-zero-party-data/ [last accessed 16/02/23]
32 Apple. Differential Privacy. No date. Available at: https://www.apple.com/privacy/docs/Differential_Privacy_Overview.pdf [last accessed 16/02/23]
33 ICO. Age appropriate design: a code of practice for online services. No date. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/ [last accessed 16/02/23]

have clear means of redress. More robust and effective enforcement of regulation is needed: likely requiring greater levels of investment in and resourcing of regulators.

- **Public education campaigns and supporting greater digital literacy education in order to promote understanding of online privacy**. At the moment, digital literacy campaigns are often left to big tech companies. While there are plenty of useful, relevant ideas in these provisions, relying on existing monopolies to deliver this information risks trapping citizens in a company's digital ecosystems and not delivering a full picture of who harvests our data, what is being collected and for what means. Other stakeholders, such as governments and civil society, are in a position to deliver public digital literacy campaigns that centre digital rights and how citizens can be empowered to assert them through the use of, for instance, data deletion schemes and tools. Teachers should also be given more support and resources for delivering digital literacy curricula to children.
- **Developing standards for privacy architecture, improving the user experience of interventions such as cookie banners**. There are inconsistencies in how individuals interact with the mechanisms meant to help keep their data transparent and within their control, inconsistencies that start with the variety of cookie banners deployed on websites that are often poorly designed, confusing and frustrating for users. Developing standards to improve the privacy architecture throughout the processes would make it more simple for organisations to implement processes that are easy and user-friendly to navigate while protecting privacy and empowering users.[34]
- **Developing standards and a process for researcher access to data**. At the EU level, the Digital Services Act includes provisions[35] which enable vetted researchers to access data from major online platforms. Allowing researcher access improves transparency around how platforms operate and the ability to understand the nature of online harms: but is often associated with worries about whether that data will be used ethically, especially following the Cambridge Analytica scandal. Where standards and an access process are developed, research capabilities can be protected in ways that protect user privacy.
- **Develop minimum standards and guidance** for how companies, particularly small businesses, seeking to comply with regulation (such as the likely forthcoming Online Safety regulations) can do so in a privacy-preserving way - for instance, how to comply with child safety duties while protecting children's and adults' privacy.
- **Protect simple ways that users can protect themselves online like end-to-end encryption and VPNs**. These are easy tools that allow users to protect against unwanted data harvesting and privacy infringements in the context of a wider ecosystem often designed to do the opposite. However, often they are portrayed as threats to citizens' safety: failing to acknowledge how removing these tools leaves citizens vulnerable to harm.

THE FUTURE

A new story for privacy

However, even if these short term measures are taken, the current system is still built on a bed of sand. More transparent cookie banners, better enforcement of data protection and wider rollout of digital literacy programmes will not shift the power asymmetries at the core of the problems caused by the current data ecosystem. Our roundtable discussions examined how short-term interventions need to be complemented by a long-term vision that could fundamentally change our expectations of privacy for the better.

It is difficult to elucidate the harm caused by undermining privacy within the 'status quo' vision. If

34 CDEI. Active Online Choices: Designing to Empower Users. No date. Available at: http://www.bi.team/wp-content/uploads/2020/11/CDEI-Active-Online-Choices-Update-Report-FOR-PUBLICATION-2.pdf [last accessed 16/02/23]
35 Albert, John. A guide to the EU's new rules for researcher access to platform data. *Algorithm Watch*. 07/12/22. Available at: https://algorithmwatch.org/en/dsa-data-access-explained/ [last accessed 16/02/23]

our relationship with data is indeed merely transactional and individual: something we own and can exchange for goods and services, then it is hard to see why that might be damaging in and of itself, beyond individual cases of abuse or fraud.

But even if every aspect of the 'status quo' approach to data worked as intended (compliance with all legal obligations, users informed and consenting to data collection), the fundamental infrastructure problem would remain - that our digital world is designed to exploit and monetise our online lives in ways that undermine our individual and collective privacy, safety and security.[36]

We need a new story and vision for data privacy: one designed with and for users, and with new champions in industry, governments and civil society.

What would this vision include?

This vision would need to recognise that the 'status quo' vision of personal data and privacy isn't working.

'Personal data' is not one entity, and that consent to use it may change in different contexts and evolve over time. Data is multiple and contextual, and rather than assuming the same model for every kind of data, we need to be differentiating[37] between data collected that relates to official-data (such as name, address, data of birth), privy-data that is the type generated as we use the internet, and collective data that contributes towards a well-defined data commons that can be used, as an example, for scientific research. The context[38] that data operates in should be recognised alongside the information it contains, which helps to explain why the level of data sharing and privacy a user agrees to changes based on the website, purpose and who they are sharing them with.

Moreover, the current emphasis on consent at the point of collection, rather than thinking about continuous consent, means understanding what later happens to data and the risks associated with data processing becomes obscured.

Privacy also expands beyond only data protection, and intersects with the enjoyment of other rights. We need a more holistic approach when discussing data privacy that recognises this: such as recognising the intersections between privacy rights, and human rights, including children's rights, commitments more widely.

Crucially, there is a *collective* discussion[39] to be had about privacy and uses of personal data, in addition to how individuals relate to and control their own data.

There are individual failures and successes within existing data protection systems, but a lack of momentum for the overall system to change in ways that benefit the public good and protect citizens' rights. This overlooks how personal data is interconnected,[40] and individual data is most useful and valuable - and monetizable - in the context of larger datasets.

This also means that individual resolutions need to be accompanied by collective forms of redress and protections. Being directed towards something once based on targeted advertising is unlikely to cause harm or significant behavioural change. It is the scale at which this gathering of information to shape decisions about our lives and to change our behaviour is where the bulk of the problem lies. Establishing mechanisms for collective redress for these harms would be another way to deepen the recognition that this is a collective problem.

Working towards this vision also means working towards technologies that embed these values in their design, so that data runs through infrastructure designed to work for the best interest of the individual

36 Tisne, Martin. Collective data rights can stop big tech from obliterating privacy. *MIT Technology Review*. 25/05/21. Available at: https://www.technologyreview.com/2021/05/25/1025297/collective-data-rights-big-tech-privacy/ [last accessed 16/02/23]
37 Snower, Dennis and Paul Twomey. Implementing an Individual-Empowered Data Governance Regime. *The New Institute*. 24/05/22. Available at: https://thenew.institute/en/media/the-case-for-collective-action/data-revolution [last accessed 16/02/23]
38 Nissenbaum, Helen. Privacy as Contextual Integrity. Washington Law Review. 2004. Available at: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10 [last accessed 16/02/23]
39 Sheppard, Emma. Data privacy is a collective concern. Open Data Charter. 14/10/20. Available at: https://medium.com/opendatacharter/data-privacy-is-a-collective-concern-8ebad29b25ce [last accessed 16/02/23]
40 Véliz, Carissa. Privacy is a collective concern. The New Statesman. 22/10/19. Available at: https://www.newstatesman.com/science-tech/2019/10/privacy-collective-concern [last accessed 16/02/23]

and society.

It is crucial that businesses, governments and civil society all play a role in championing the development of this future vision.

Businesses can take the following steps:

Invest in developing and deploying privacy-preserving infrastructure

To move away from a model in which privacy regulation has to always act as a handbrake on the excesses of current technologies, we need to move towards a model that has privacy as the default, and designing and adopting technologies that imbed the values we want from data in their design as standard. This should involve companies engaging with privacy and rights experts throughout the design and development process of new technologies, and support with conducting e.g. privacy impact assessments.[41]

There are multiple exciting possibilities for these kinds of technologies emerging.

- Data pods, for instance, reimagine how data is managed: rather than being in control of the websites that collect it, data is kept in decentralised stores controlled by the data subject. Access to this data can then be granted or revoked by the user to organisations requesting access. Pods are not without their own problems - they require a level of technical engagement and understanding from the user, and there is yet to be a way of preventing the organisations accessing data from simply making their own copy - but represent ways of thinking about data and associated standards that centre privacy, autonomy and control.[42]
- Privacy Enhancing Technologies (PETs) are a collection of tools[43] that reduce the risks that come with working with data while still maximising data's usefulness. Approaching privacy through a suite of tools is one way to embrace the multiplicity of the purposes of data, and is a particularly promising route to access the social good of research on collective data. Examples of PETs currently being experimented with by social media platforms include homomorphic encryption[44] (where computation can be performed directly on encrypted data) and federated learning[45] (where datasets are broken up and machine learning algorithms are trained in a distributed manner). PETs are an exciting route forward for research that protects individuals and benefits the collective.[46] Embedding them within social media platforms can also help safeguard data; however they do not inherently disrupt the business model of social media platforms.

Meanwhile, governments can:

Apply a privacy lens to all areas of digital regulation to maximise the opportunities for change:

There is a host of forthcoming regulation that seeks to tackle digital challenges, from online harms to monopoly power. Putting privacy as a key priority of these regulations would help support a holistic and consistent regulatory framework that would help tackle the structural challenges of digital privacy from many different angles.

41 Ibid.
42 Solid Project. Solid Protocol. 17/12/21. Available at: https://solidproject.org/TR/protocol [last accessed 16/02/23]
43 The Royal Society. From privacy to partnership: The role of privacy enhancing technologies in data governance and collaborative analysis. 2023. Available at: https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/From-Privacy-to-Partnership.pdf [last accessed 16/02/23]
44 Wikipedia. Homomorphic encryption. No date. Available at: https://en.wikipedia.org/wiki/Homomorphic_encryption [last accessed 16/02/23]
45 Open Data Institute. Federated Learning: an introduction. 2023. Available at: https://www.theodi.org/wp-content/uploads/2023/01/ODI_Federated-learning_-an-introduction-%E2%80%93-Considerations-and-practical-guidance-for-prospective-adopters-report.pdf [last accessed 16/02/23]
46 CDEI. Winners announced in first phase of UK-U.S. privacy-enhancing technologies prize challenges. 10/11/22. Available at: https://www.gov.uk/government/news/winners-announced-in-first-phase-of-uk-us-privacy-enhancing-technologies-prize-challenges [last accessed 16/02/23]

- **Tackle surveillance advertising model through regulation similar to the Digital Services Act**. At the heart of the current systems of data collection is the surveillance model system, where data is harvested and sold on in opaque ways in order to sell audiences to advertisers. Following the DSA, the UK government could disrupt the surveillance advertising processes by ensuring that information used to target users with adverts is disclosed[47] with the advert, and introducing mandatory transparency reporting[48] on algorithms to understand how data is being used.
- **Use the forthcoming Digital Markets regulation as another vehicle for challenging the tech monopolies** which rely on data-driven business models. The new Digital Markets Unit[49] will be tasked with setting out pro-competitive requirements for companies designated as having 'strategic market status' and making interventions where necessary - such as those which could promote greater interoperability. The work of the Unit should include identifying where pro-competitive interventions could also better promote privacy-first practices.
- **Use the opportunity of the new Data Reform Bill to ensure strong data protection regulation that centres the needs of citizens**. This should include both individual and collective right to understand the decisions of automated processes, and creating a special status for children's data. The Bill also offers an opportunity to improve the means[50] by which individuals or collective groups can bring a complaint against an organisation's handling of data to the ICO.
- **Use regulation to improve the transparency and accountability of AI and the algorithms used to process and analyse the vast quantities of data collected.** What is done with our data once collected is a crucial area of risk. The EU's AI Act[51] takes a risk based approach to assess the level of risk posed by different systems. Some AI systems covered by our research, notably credit scores, are counted as high risk and will be required to meet certain obligations such as risk assessments, logging activity, user transparency and having a level of human oversight. Even where risk is low, users need to be clear that they are interacting with a machine. These rules apply equally to government AI systems, the use of which should be made much more transparent to the public. However, these rules do not go far enough[52] in centering the rights of those impacted by AI systems and recognising AI as often a series of interlocking, dynamic systems. Future AI regulation needs to start from this complexity and centre the rights of users impacted.

The next general election in the UK will be within two years. This also represents a significant political opportunity for all parties to develop a collaborative vision for what data privacy in 2025 could and should look like: through in-depth, meaningful engagement with citizens, civil society, and industry to move closer to a collective understanding of how both the benefits of data-driven technologies and protecting privacy can be realised in a digital age.

Other steps require governments, businesses and civil society to work together, such as:

Develop new standards to promote interoperability and privacy-preserving data flows

- Other proposals put forward a more radical overhaul of information management. *How the Web Should Work*, a project led by Demos Fellow Jon Nash, proposes a three-prong approach to improve our data infrastructure. This would include introducing:

47 Dentons. The DSA: Consequences of the use of digital advertising. 30/08/22. Available at: https://www.dentons.com/en/insights/articles/2022/august/30/the-dsa-consequences-of-the-use-of-digital-advertising [last accessed 16/02/23]
48 The Verge. Google, Meta, and others will have to explain their algorithms under new EU legislation. 23/04/22. Available at: https://www.theverge.com/2022/4/23/23036976/eu-digital-services-act-finalized-algorithms-targeted-advertising [last accessed 16/02/23]
49 BEIS and DCMS. A new pro-competition regime for digital markets - government response to consultation. 06/05/22. Available at: https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets/outcome/a-new-pro-competition-regime-for-digital-markets-government-response-to-consultation [last accessed 16/02/23]
50 Freegard, Gavin. Ensuring People Have a Say in Future Data Governance. *Connected by Data*. 06/12/22. Available at: https://connectedbydata.org/events/2022-12-05-data-protection-digital-information-bill-parliamentary-event [last accessed 16/02/23]
51 European Commission. Regulatory framework proposal on artificial intelligence. No date. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai [last accessed 16/02/23]
52 Edwards, Lilian. Expert opinion: Regulating AI in Europe. *Ada Lovelace Institute*. 31/03/22. Available at: https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/ [last accessed 16/02/23]

- ‘Standardised requests: organisations needing to collect personal data to carry out their function (such as a service taking payment from a customer) would do so via specific, data-minimising and standardised requests. The technical standards for this should be set out by an independent standards body to ensure interoperability.
- Licensed organisations: the organisations who were able to make these specific requests would be licensed to ensure the credibility of those who were sending and receiving personal data.
- Routed with user consent: there would be a clear, standardised way of securing user consent before information was passed between organisations.’[53]

This proposal would mean that a user’s OS provider would route requests for information through routing questions and answers between organisations which hold the necessary information and organisations requiring it, rather than the user themselves having to enter information in multiple places. (For instance, a bank providing a ‘yes’ or ‘no’ in response to the question ‘does this user have a UK bank account’, rather than needing to share all of the users’ bank details directly with the organisation raising the query.)[54]

This would need ‘standards backed by an independent body to protect individuals’ privacy while making the necessary data accessible and useful to those who it should be shared with.’[55] The trade off with this vision[56] is a rise of frictionless design that can leave some internet users more at risk than others.

53 Nash, Jon. 2023.
54 Nash, Jon. 2023.
55 Nash, Jon, 2023
56 Coldicutt, Rachel. Easy to use but hard to understand: moving beyond the pitfalls of frictionless digital design. *Medium*. 13/01/23. Available at: https://rachelcoldicutt.medium.com/easy-to-use-but-hard-to-understand-moving-beyond-the-pitfalls-of-frictionless-digital-design-ca622011324f [last accessed 16/12/23]

CONCLUSIONS

The scale of data held about us is near-impossible to grasp. This challenge is significant: it means that the legal tools meant to empower citizens instead too often fall short, demanding huge amounts of time and effort from individuals to even scratch the surface of the data that is held about them. Individuals are unable to control their data or give meaningful consent to how it is used, and do not know the extent of what is being collected, while the purposes it is used for remain opaque. Even in the face of harm, redress mechanisms are inadequate and not accessible to all.

It is clear the current landscape for data protection is not working. To fix this it is going to be essential to step away from seeing solutions at the level of individual actions, about which cookies they do or do not accept, about which web services they do or do not access. Instead, businesses, alongside strong regulatory action from governments, need to take seriously their responsibility to crafting a data ecosystem where the potential of data can be realised without compromising individuals' right to privacy.

Some of this work is short-term and can be done now. Businesses can champion privacy by taking advantage of new ad-tech that relies less and less on buying personal data and making their systems clear and accessible for individuals. Governments can enforce existing regulation better and develop standards designed to protect citizens.

But for real change to occur, businesses, governments and civil society need to pursue a new vision for data; working together to develop new privacy-preserving infrastructure that recognises the contextual nature of data, the intersection of privacy with other rights and the collective nature of the information held about us.

APPENDIX

		% COMPANIES RESPONDING TO DATA DELETION REQUESTS				
		Volunteer A	Volunteer B	Volunteer C	Volunteer D	Volunteer E
Overall Companies Responded*		57	10	33	46	65
Of those who responded, they…	Automated response with no-follow up	8	1	7	4	6
	Replied with timely, relevant responses	49	9	26	42	59
Of those who replied with timely, relevant responses, their response was…	Complied immediately	30	3	11	13	25
	Number of self-service portals	2	1	3	0	3
	Entitled to maintain	3	0	2	8	0
	Asked for further info	2	4	2	4	17
	Redirect to privacy portal	0	0	0	0	8
	No relevant info	13	1	5	8	6
	Sent to a different department	0	0	3	4	0

From data provided by Rightly

** Responses within time period of Rightly research: first volunteer onboarded 7 April, end date 5 August 2022.*

Licence to publish

Demos – Licence to Publish

The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions

a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.

b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.

c 'Licensor' means the individual or entity that offers the Work under the terms of this Licence.

d 'Original Author' means the individual or entity who created the Work.

e 'Work' means the copyrightable work of authorship offered under the terms of this Licence.

f 'You' means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights

Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant

Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:

a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b to distribute copies or phono-records of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions

The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phono-record of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder. You may not sublicence the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

c If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, you must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

a By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:

i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;

ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

b Except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an 'as is' basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination

a This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.

b Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

a Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.

b If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

c No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

d This Licence constitutes the entire agreement between the parties with respect to the Work licenced here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of Demos and You.

DEMOS

Demos is a champion of people, ideas and democracy. We bring people together. We bridge divides. We listen and we understand. We are practical about the problems we face, but endlessly optimistic and ambitious about our capacity, together, to overcome them.

At a crossroads in Britain's history, we need ideas for renewal, reconnection and the restoration of hope. Challenges from populism to climate change remain unsolved, and a technological revolution dawns, but the centre of politics has been intellectually paralysed. Demos will change that. We can counter the impossible promises of the political extremes, and challenge despair – by bringing to life an aspirational narrative about the future of Britain that is rooted in the hopes and ambitions of people from across our country.

Demos is an independent, educational charity, registered in England and Wales. (Charity Registration no. 1042046)

Find out more at **www.demos.co.uk**

DEMOS

PUBLISHED BY DEMOS MARCH 2023

15 WHITEHALL, LONDON, SW1A 2DD
T: 020 3878 3955
HELLO@DEMOS.CO.UK
WWW.DEMOS.CO.UK

SCHILLINGS

RIGHT TV