ECONOMIST IMPACT

Open access: the future of data portability

Sponsored by AMBER

Contents

3 About this project

4 Executive summary

6 Introduction: a moment of reckoning

8 Data portability complexities

11 The legislative landscape

16 New age architecture

20 The consumer perspective

31 Conclusion

33 Methodology and demographics

About this project

Open access: the future of data portability is a report by Economist Impact. It explores the findings of a global survey of over 1,500 consumers and interviews with ten data legislation, management and portability experts. This report considers the growing importance of data portability for consumers, businesses and societies globally, explores the legislative landscape for data portability at present, and examines consumer perceptions regarding data portability and potential data portability models.

The programme is sponsored by Amber Group. The Economist Impact research team comprised Piotr Zembrowski, Alexander VanKemenade, Divya Sharma and Shreyansh Jain. The report was written by Georgia McCafferty and Ed Wright, and edited by Piotr Zembrowski. Economist Impact would like to thank the survey participants and the interviewees who generously offered their time and insights, in particular:

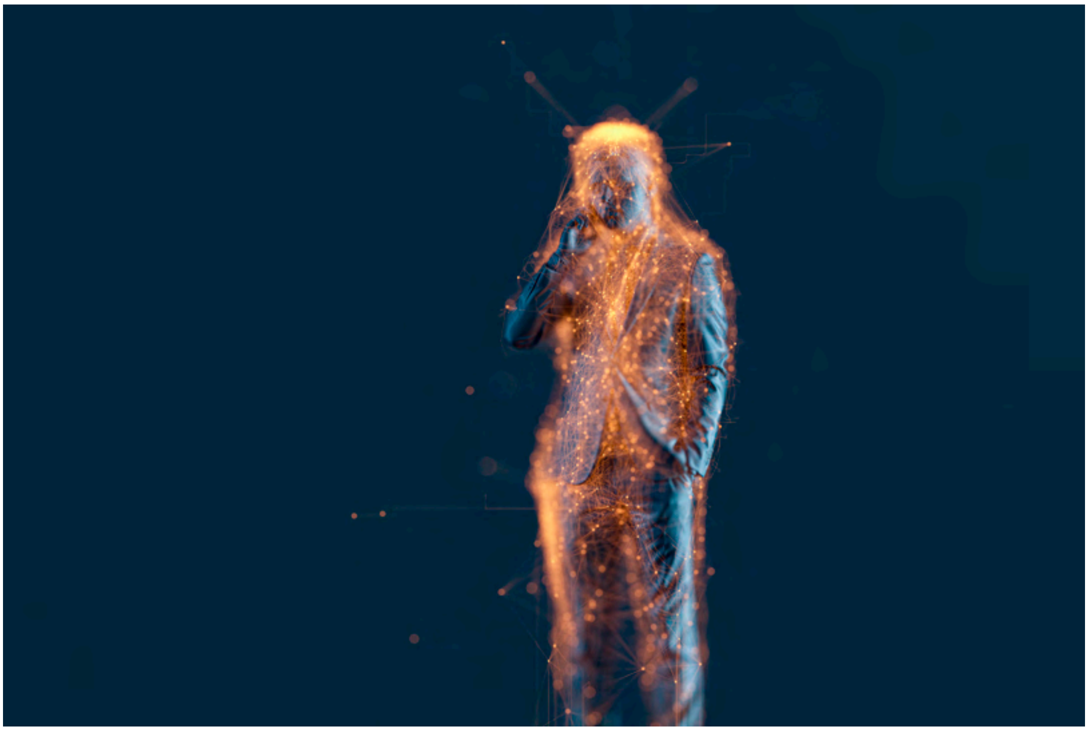
- Michael Sena, co-founder and CEO, 3Box
- Ross Buckley, Scientia professor, School of Private & Commercial Law, the University of New South Wales
- Wayne Chang, co-founder and CEO, Spruce Systems
- Alexander Cardona, co-founder and COO, Codat
- Ryan Budish, data portability specialist, Meta
- Ali Lange, privacy manager, Google
- Gail Hodges, executive director, Open ID Foundation
- Peter Swire, professor of law and ethics, Georgia Tech Scheller College of Business
- Inge Graef, associate professor of competition law, Tilburg University

The findings and views expressed in this report are those of Economist Impact and do not necessarily reflect the views of survey respondents, interviewees or the project sponsor.

Executive summary

As technology evolves from a platform-based approach to distributed technology architecture, data portability is becoming a vital capability. It will provide consumers with greater choice and remove some of the friction that comes with traditional platform-based systems. However, while the concept is simple, there are many challenges to achieving user-friendly data portability.

Aside from technological hurdles, which are likely to be overcome as digitalisation progresses, a significant challenge is the lack of awareness of data portability among consumers. Many users have needed to transfer their data from one provider to another (most often between different mobile phone companies) but most have an almost apathetic approach to data security, which is a critical component of



effective data portability.

Large parts of the world also lack effective data legislation. Where effective data legislation is in place, many regulators have taken a relaxed approach to enforcing data portability rights or used it as an antitrust tool rather than a consumer-focused right. As a result, most businesses lack the impetus they need to facilitate data portability and have not taken appropriate steps to adapt.

Meanwhile, consumers, regulators and businesses all face a fast-changing landscape. As new distributed-ledger technologies like blockchain gain momentum, Web3—a new generation of decentralised internet—is emerging, and digital assets are poised to enter the mainstream. This will require legislative flexibility and new, more intuitive data portability tools, which can help consumers, and the businesses that serve them, adapt to a new digital reality.

The key findings from this project are:

- **Data portability will soon become a necessity.** Web3 technologies and the growth in distributed technology systems like cloud computing have the potential to radically change the demand for data portability. Regulations will need to become more flexible while data portability tools need to become more user-friendly and sophisticated.
- **Achieving data portability is complex.** When implemented in a considered, measured manner, data portability can bring a wealth of benefits to businesses and consumers. These include a wider choice of suppliers and service providers and more control over the way their data are used. But there are many significant technological barriers to overcome before achieving this.
- **Data portability regulation is not an antitrust tool.** Policymakers need to strike a balance with data portability regulations that are designed around the needs of consumers and businesses, as well as competition. Regulators also need to help businesses understand the impact of data portability rights and help them adapt in response, so these rights can be more effectively enforced.
- **Consumer awareness of the need for data portability is low.** Over two-thirds (70.5%) of global consumer respondents have not read about data privacy laws in their country or state and only 10% say they have requested a transfer of their personal data from one service provider to another.
- **Consumer attitudes towards trust do not always lead to action.** There is no correlation between the trust (or lack thereof) that consumers have in how their data are handled by institutions and the actions they take to mitigate their personal data security risk. People may be mistrustful of how internet platforms use their personal data, but they often do very little to address this.
- **Data-portability cannot be achieved by regulation alone.** Although a simple concept, the technical realities of data portability—including transparency, conformity and security concerns around data that have been transferred—mean that new ways of enabling data portability need to be explored. At present, the technology isn't sufficiently developed to bring consumers to the tipping point of adoption.

Introduction: a moment of reckoning

For Wayne Chang, co-founder and CEO of Spruce, a decentralised identity software company, the realisation that someone else had control over his online data was "deeply unsettling". Having used the internet for most of his life, it was not until his late teens that he understood that a large part of what he believed was his actually belonged to someone else.

"My personal identity is actually tied with my digital identity, so it felt pretty offensive when I learned that my information is being disclosed in a certain way without my consent," he explains. "For some people the internet is Facebook—for me, it is an extension of my life."

This personal consideration of data sharing—and the significant impact it has for businesses and consumers globally—was highlighted by large-scale data hacks in Australia in late 2022. The first company to be impacted was Optus, Australia's second largest telecommunications provider.

The security breach saw an individual gain access to the personal data of up to 10 million Optus customers—or approximately 40% of Australia's population—including names, birth dates, phone numbers and email addresses. For some customers, passport numbers, drivers' licence details and Medicare numbers were also stolen, exposing them to potential identity theft.

Just a few weeks later, in what appeared to be a case of déjà vu, Medibank Private, one of Australia's largest private health insurers with almost 4 million customers, announced that it too had been hacked, this time by a co-ordinated organisation. Data, including people's names, phone numbers and, in some cases, medical histories and identifying documents, were subsequently published on the dark web.

The consumer, government and legal backlash to the leaks, and how the companies managed the aftermath, was immediate and extreme. It intensified further when previous customers of both Optus and Medibank realised that their data, which had been stored by the companies despite them not having used such services for five years or more, had also been stolen.

Described as "a moment of reckoning for Australian businesses",[1] it is estimated that both companies will lose millions[2,3] from the costs of compensation, security system rectification, class action lawsuits, and the loss of existing and potential customers.[4] Yet the fallout from these data hacks is indicative of a broader challenge for companies globally.

The rapid digitalisation of the past five years has transformed business models. However, companies now need to navigate a further digital transition where systems become decentralised, at a time when Web3 is fast materialising and data is taking on a life of its own. Many find themselves ill-equipped to manage and protect data as technology changes, and face the triple threat of punitive fines or legal cases for mismanagement, growing regulatory oversight and increasingly loud consumer concern.

Consumers face similar challenges. As technology and the internet have become ubiquitous to business, governments and societies, many have found that their real-world and data-driven digital identities are converging. The emerging fifth industrial revolution (5IR) promises even closer collaboration between humans and technology,[5] and with developments like Web3 and the metaverse on the horizon, the present distinction between people's digital and real identities becomes more tenuous.

Through their impact on fundamental economic and societal functions, these challenges also raise much larger questions concerning the ownership of data and its portability. How aware are consumers and businesses of the ownership of their data and the potential to take back ownership? What are the best models to facilitate this type of data ownership and the data portability that it enables? What present regulatory systems facilitate this and how effective are they? And how could future technological and data portability changes impact economies globally?

[1] How the Optus breach will change corporate Australia forever, Paul Smith and John Davidson, Australian Financial Review, September 30th 2022, https://www.afr.com/technology/how-the-optus-breach-will-change-corporate-australia-forever-20220929-p5bm1p

[2] Giant Optus Hack May Swallow a Quarter of Singtel Profits, Angus Whitely, Bloomberg, September 29th 2022, https://www.bloomberg.com/news/articles/2022-09-29/giant-data-hack-in-australia-risks-eating-into-singtel-s-profit

[3] Medibank Hack Could Cost A$700 Million in Compensation, Fixes, Bloomberg, November 10th 2022, https://www.bloomberg.com/news/articles/2022-11-10/medibank-hack-could-cost-a-700-million-in-compensation-fixes

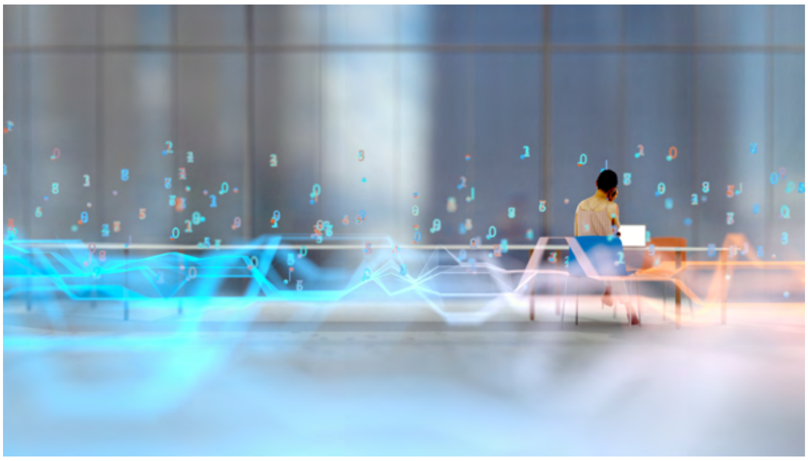
[4] The Optus hack will cost millions (and not just in payouts), Chanticleer, Australian Financial Review, September 22th 2022, https://www.afr.com/chanticleer/the-optus-hack-will-cost-millions-and-not-just-in-payouts-20220923-p5bkkm

[5] The Fifth Industrial Revolution: How harmonious Human-Machine Collaboration is Triggering a Retail and Service (R)evolution, Stephanie M. Noble, Martin Mende, Dhruv Grewal, A. Parasuraman, Journal of Retailing, June 2022, https://www.sciencedirect.com/science/article/pii/S0022435922000288

Data portability complexities

Data portability, or the capacity for individuals or businesses to easily control and move data between different applications, platforms, programs or computing environments, has long been a topic of debate among technology companies. However, for the broader public, it is an underappreciated concept—or a right in some countries—that is growing in importance as technology advances and the role of data in fuelling global economies evolves.

As a right and a technology concept that is tied closely with data protection, data portability has many benefits for businesses and consumers because it gives people greater control of how their data are used and who can use it. In a practical sense, that makes it easier to switch between providers, thereby avoiding vendor lock-in and encouraging competition—which in turn increases choice, reduces switching costs and makes the integrity of data more resilient.[6]



"It's a tool of empowering consumers or businesses to move their data elsewhere. When data portability is managed well, it can also lead to more competition for services, so it's good for society overall," explains Inge Graef, associate professor of competition law at Tilburg University.

The concept of data portability first gained prominence in 2008 when Yahoo, MySpace, Google, Microsoft and Facebook (now Meta)—among others—participated in a Data Portability Workgroup, which aimed to create a way for people to easily share and move their data between social media profiles and other applications.[7]

The group's work formed the basis for many present-day data portability approaches, but it

[6] Data Portability, Interoperability and Digital Platform Competition, OECD Competition Committee Discussion Paper, OECD, 2021, https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf

[7] The New Portability: Designing Portability with Competition in Mind, Nicholas, Gabriel, Engelbert Center on Innovation Law and Policy, NYU School of Law, August 2020, https://www.law.nyu.edu/sites/default/files/The_New_Data_Portability.pdf

failed to gain consensus on a unified model. One of the main reasons for this is that while data portability is relatively simple to understand, it can be exceedingly hard to implement. Once achieved, it can also have unintended consequences.

The need for conformity

One of the key challenges to data portability is conformity, as it requires data to be stored in a commonly recognised format. Yet the way data are collected, stored, managed and protected varies enormously between systems and organisations, which creates compatibility problems. To overcome this problem, technology companies have created tools that translate one organisation's data so that it can be understood by another. Yet these tools, called application programming interfaces (APIs), also need to be standardised to facilitate this.[8]

Comparison of data points also relies on standardisation, which requires agreement on definitions. Ross Buckley, a Scientia professor in the School of Private & Commercial Law at the University of New South Wales, says achieving the level of standardisation required to facilitate data portability can itself be a mammoth task.

"For instance, an example in Australia that shows the minutiae of this problem, is that a flood is defined differently by different insurance companies—whether it's coming from the sky, from a storm, or if it's the result of rising from a river. The industry is going to have to agree about that. Otherwise you're not going to be able to compare data from flood insurance policies," he explains.

Data portability has many other practical nuances, including the need for data to be transparent. This can create unintended consequences in the form of security challenges. If implemented incorrectly, data portability requirements can "pose serious risks to the privacy, security and integrity of information," says Peter Swire, a professor of law and ethics at the Georgia Tech Scheller College of Business. "For access to important data, effective authentication is absolutely necessary."

Consumers need to be aware of and understand how to use data portability to help them switch services,[9] and recognise the potential security consequences once they have ported their data. Ali Lange, a privacy manager with Google in California, says this is one of Google's most significant concerns with its data portability tool, as the security of the data becomes the consumer's responsibility once it has been ported.

"When you're talking about typical portability, you're talking about a user exporting a copy of data from a service," says Ms Lange. "Once a user does that, the entity that originally has the data or has the first copy of the data can no longer help with security."

Legacy systems further impact the implementation of data portability. Centralised systems—where data and information are owned by and stored on a central network—are the basis of traditional IT infrastructure and hence the mainstream data management tools that are currently used today. Controlled by one sole authority or network, these systems dictate data formats and management, which add to the practical challenges around data portability and the tools that enable it.

[8] Making data portability more effective for the digital economy: Economic implications and regulatory challenges, Centre on Regulation in Europe, June 2020, https://cerre.eu/wp-content/uploads/2020/07/cerre_making_data_portability_more_effective_for_the_digital_economy_june2020.pdf

[9] The Right to Data Portability: conception, status quo, and future directions, Kuebler-Wachendorff, S., Luzsa, R., Kranz, J. et al. Informatik Spektrum, July 6th 2021, https://link.springer.com/article/10.1007/s00287-021-01372-w

Digitalisation and disruption

Despite these barriers, the rapid pace of digitalisation experienced during the covid-19 pandemic has created an urgent and growing need for data portability to become more widely available. As technology has developed and digitalisation has advanced, cloud services and architectures have become common, and systems are becoming increasingly decentralised.

This decentralised approach sees systems operate on interconnected models where no single location or entity is the sole authority. Interoperability and portability are important for these systems to be able to operate efficiently and adapt to changing technology and business needs[10] and prevent vendor lock-in.[11]

Technologies like Web3 and blockchain also operate on the idea of a decentralised approach to information. Rather than data being held on a centralised server owned by a single entity, it is stored on a distributed shared ledger. Within this, independent computers known as nodes record, share, synchronise and validate transactions.[12,13] This creates a further need for decentralised identities, which leads to the question of data portability.

"Decentralised identity is an identity system that isn't controlled by a single company or organisation," explains Michael Sena, co-founder of 3Box, a software and applications developer. "It is a system where anyone can openly register a new digital identity, can control their own identity, and can take that identity with them, so they're not trapped in any single system."

In contrast to a platform like WeChat, for example, where a user's identity exists on its servers and cannot be moved to another platform, a decentralised identity provides digital users with a single online identity that they can control and use across different platforms. "You can't really have portable data if all that data is associated with an account that's on someone else's server. So decentralisation enables decentralised identities, they are critical pieces to data exchange and data portability," adds Mr Sena.

Data are also changing due to digitalisation. The proliferation of new technologies and the 5IR will see data volumes grow at an exponential rate, while inferred or generated data—new data that are generated by a system that processes a person's original data without their express input—are also becoming increasingly important. This raises legitimate questions as to who owns the inferred data, given that the processes that work upon it are considered the intellectual property of the data user,[14] which in turn has an impact on data portability.

"Some of the foundational issues we need to solve now will set us up for success for the future," says Ms Lange of the need to address data portability in order to adapt to the changing technological landscape. "We're trying to create the opportunity for people to try new things. We're trying to keep people in control of their data. With mindfulness of the ways people actually use data portability, you can come up with answers to these problems."

[10] Cloud Portability and interoperability, Chris Nott, IBM:n Think-blogi, October 20th 2022, https://www.ibm.com/blogs/think/fi-fi/2020/10/20/cloud-portability-and-interoperability/

[11] Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective, Justice Opara-Martins et al, Journal of Cloud Computing, April 15th 2016, https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-016-0054-z

[12] "What is Web 3?, Kevin Roose, The New York Times, https://www.nytimes.com/interactive/2022/03/18/technology/web3-definition-internet.html

[13] Blockchain & Distributed Ledger Technology, World Bank Brief, April 12th 2018, https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt

[14] "Data Portability in a Data-Driven World", Frederike Zufall and Raphael Hingge in *Artificial Intelligence and International Economic Law*, Cambridge University Press, October 2021, https://www.cambridge.org/core/books/artificial-intelligence-and-international-economic-law/data-portability-in-a-datadriven-world/F445EC4A9E9665A05E773A88E8840027

The legislative landscape

As technology evolves, the need for increased data portability grows more urgent. Although relevant legislation is becoming more common, only certain markets are implementing it. Despite the importance of data protection and portability to consumers, businesses and societies, data regulation has historically lagged changes in technology.

Just 71% of the world's nations had data protection and privacy legislation in place at the end of 2021, while another 9% had draft legislation yet to be enacted,[15] according to the UN. However, the emergence of large technology monopolies—or big tech—over the past decade, and their increased power stemming from the rapid digitalisation and economic disruption created by the covid-19

[15] Data Protection and Privacy Legislation Worldwide, UN Conference on Trade and Development, December 14th 2021, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

[16] Is big tech now just too big to stomach, Jasper Jolly, The Guardian, February 6th 2021, https://www.theguardian.com/business/2021/feb/06/is-big-tech-now-just-too-big-to-stomach

pandemic,[16] has seen regulators in the US, Europe, the UK, Singapore and Australia pay more attention to these issues.

Initially, this attention focused more on data privacy, after it emerged in March 2018 that Facebook had shared users' data without their consent.[17] Data portability then became a political issue when a British publication, the Observer, revealed that Cambridge Analytica had acquired the data of up to 87 million Facebook users without their consent for use in attempts to influence elections.[18] This highlighted the lack of transparency in many organisations regarding their use and sharing of customer data, and the influence that large technology companies can have on global economies and societies. It placed these companies firmly in the regulatory firing line of Western democracies.

Regulatory reverberations

Many years in the planning, the General Data Protection Regulation (GDPR) came into effect in the EU on May 25th 2018, adding fuel to the data regulation debate. Considered to be the world's strongest data privacy and security legislation so far, it protects personal data in all EU member states, including the right to data portability. It also imposes obligations on organisations globally if they collect data related to people residing in the EU.[19]

The implementation of the GDPR heightened global scrutiny of the way large technology companies manage data. Other countries quickly followed suit with legislation that reflects the GDPR's influence.

In the US, the California Consumer Privacy Act (CCPA), which went into effect in 2020, provides greater data transparency, the right to delete, the right to opt out, and the right to portability of all personal information, among other rights.[20] The first broad data privacy law in the US, it covers medium-to-large organisations and acts as a proxy for the rest of the country, as it enables Americans in any state to reset their data relationships.[21] A national law is in development, but weak federalism and the frequently divergent positions of state jurisdictions have caused legislative complexity.

Singapore passed its Personal Data Protection (Amendment) Bill in November 2020,[22] which updated existing data protection legislation. However, the data portability obligation within the new bill has not yet been enacted, and no date has yet been announced for what is planned to be a phased implementation.[23]

Australia currently has no universal right to data portability. The Consumer Data Right (CDR) was introduced in July 2020 to enhance data portability and increase competition by reducing customer lock-in. It is in the process of being rolled out on a sector-by-sector basis, starting with banking.[24]

[17] Big tech is growing, but so is investors' caution, The Economist, April 26th 2018, https://www.economist.com/business/2018/04/26/big-tech-is-growing-but-so-is-investors-caution

[18] Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users, The New York Times, https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html

[19] What is the GDPR, the EU's new data protection law, GDPR.eu, https://gdpr.eu/what-is-gdpr/

[20] California Consumer Privacy Act (CCPA), State of California Department of Justice, 2018, https://oag.ca.gov/privacy/ccpa

[21] Don't sell my data! We finally have a law for that, Geoffrey A. Fowler, The Washington Post, February 19th 2020, https://www.washingtonpost.com/technology/2020/02/06/ccpa-faq/

[22] Data Protection Obligations, Personal Data Protection Commission Singapore, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[23] Upcoming changes to the PDPA: Introducing Data Portability, PK Wong & Nair, October 26th 2022, https://pkwongnair.com/2022/10/26/upcoming-changes-to-the-pdpa-introducing-data-portability/

[24] What is CDR? Consumer Data Right, the Australian Government, https://www.cdr.gov.au/what-is-cdr

After formally leaving the EU in January 2020, the UK kept the GDPR in force as the UK GDPR.[25]

Consumer empowerment or antitrust?

Existing legislation tends to emphasise the right to data privacy and the ability of individuals to access the data that companies hold about them. Data portability has been an afterthought or is enforced more as an antitrust tool to encourage competition among big tech and social media companies.

Ryan Budish, a public policy manager at Meta, says that in the markets where legislation exists, data protection and data portability are rights. But Ms Graef says many data regulators, acknowledging the technical challenges with implementing data portability, have instead placed the issue into the "too hard basket".

Even the GPDR, which enshrines the right to data portability in Article 20[26] and carries heavy penalties, has not yet had a significant impact on data portability in practice, according to Ms Graef.

"When the GDPR was introduced, there was a lot of expectation on these new rights, but while it has had a significant impact in other areas, nothing is yet happening with enforcement of portability," she says. "There's a lot of potential, especially now there is a growing belief that we should move more towards an open internet again, where a consumer controls where the data goes and who has access to it. But there's been no action."

Part of the issue is that without enforcement, there is no impetus for businesses to respond. Many also argue that although regulations like the GDPR control the 'negative right to data'—which prevents organisations from sharing personal data with third parties without the data owner's permission—it has not yet focused enough on the 'positive right'. This refers to enabling people to move their data between service providers and from platform to platform.

Mr Swire says the premise that underlies most present data regulations—that if the data being stored are about an individual, it is their right to move these data to another service—is well accepted in Europe, the US, the UK, Australia and Singapore. But the way that the regulations are implemented tends to be done with the sole intention of improving competition rather than enforcing that right.

"Data portability is an expression of autonomy," he says. "What gets harder is when the antitrust experts want to blow open the databases of big tech companies to foster competition. And they don't always understand the privacy and cybersecurity risks that come with it."

Ms Lange agrees and says that for regulation or policy to succeed in encouraging data portability, its proponents need to understand consumer behaviour and motivations, and not use it solely to encourage competition. She says that regulators are aware of the work and large investments that companies like Google and Meta have expended over many years to create data portability tools.

But because implementing data portability is still a challenge for smaller companies, she says many policymakers focus on it as a tool that encourages moving consumers from a large

[25] Overview - Data Protection and the EU, Information Commissioner's Office, https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/

[26] General Data Protection Regulation, 2016/679, GDPR, https://gdpr-info.eu/

platform to a small one rather than something with greater applications that can benefit businesses and consumers alike. "Using data portability as a punishment for being too big misunderstands the entire purpose of data portability," Ms Lange says.

Ms Graef says this illustrates one of the core issues of data portability policy—that it encompasses different objectives. "It's about consumer empowerment. It's also data protection. But because of the link with competition and innovation, it's hard to see who should be in charge and under which policy exactly it should fall," she explains.

The rapid pace of technological development also makes it hard for policy to keep up. Mr Buckley says that regulators are in a difficult position of trying to provide frameworks for new technologies without discouraging their development while trying to retrofit legislation to wind back some of the market domination achieved by the major Web2 platforms.

This creates further challenges, as observed data—like tracking cookies that record browsing—and inferred data grow at an exponential rate as technology develops. However, at present, existing legislation does not specify the kind of personal data that people should have the right to port and, as with the GDPR, only regulates portability for data voluntarily provided by the user.[27] This basic definition applies to social media posts and simple consumer data but not more complicated data types.

This can seem like an oblique problem, but it has real world issues. Skimmed and inferred data can be used to construct credit scores, for example, or calculate insurance premiums.[28] And as digital

The Data Transfer Project

The success of data portability regulation ultimately rests upon the technical feasibility of moving data easily between platforms, which is difficult to achieve. To help solve this, Google, Meta, Microsoft, Apple and Twitter formed the Data Transfer Project (DTP) in 2018 to build an "open-source, service-to-service data portability platform so that all individuals across the web could easily move their data between online service providers whenever they want."[29]

The DTP statement of data portability is focused on consumer experience, on providing people with the ability to easily switch between products and services, and on the security benefits from being able to back up or archive information.[30] "We think the DTP is a tremendously exciting way to help build integrations between companies so that they can enable more effective portability," says Ryan Budish, a public policy manager at Meta.

To achieve this, DTP has developed an open-source framework with three tools that facilitate data portability: data models, adapters and a task management library. This enables any business to write an adapter, which can then be used to export or import data in a data model via the DTP. In essence, the DTP functions as an intermediary by which a data owner can transfer their data from one platform to another.[31]

The development of the DTP has been gradual, despite significant investments of time and money by the alliance companies, and although it has enabled users to download data from a platform, the technical challenges with data portability remain an issue, even where the will to actualise data portability is strong.[32] Ali Lange, a privacy manager with Google, says interoperability is the main challenge and many people are committed to solving it.

Yet a larger issue with social media data portability may remain regulatory, according to Mr Swire, because the data are not just about one person but their contacts as well. "It's very hard to create a consent structure that enables social media portability with the agreement of all one's friends and family," he says.

[27] "Data Portability in a Data-Driven World", Frederike Zufall and Raphael Hingge in *Artificial Intelligence and International Economic Law*, Cambridge University Press, October 2021, https://www.cambridge.org/core/books/artificial-intelligence-and-international-economic-law/data-portability-in-a-datadriven-world/F445EC4A9E9665A05E773A88E8840027

[28] Insurance firms can skim your online data to price your insurance – and there's little in the law to stop this, Zofia Bednarz, Kayleen Manwarring and Kimberlee Weatherall, The Conversation, June 20th 2022, https://theconversation.com/insurance-firms-can-skim-your-online-data-to-price-your-insurance-and-theres-little-in-the-law-to-stop-this-185038

[29] See: https://datatransferproject.dev

[30] See: https://datatransferproject.dev/dtp-overview.pdf

[31] Data Transfer Project: Enabling portability of photos and videos between services, Engineering at Meta, December 2nd 2019, https://engineering.fb.com/2019/12/02/security/data-transfer-project/

[32] Google Pledges More Investment in for Data Transfer Project, March 12th 2022, https://timesofindia.indiatimes.com/gadgets-news/google-pledges-more-investment-in-for-data-transfer-project-what-it-is/articleshow/90206126.cms

assets become mainstream, the data legislation landscape will grow even more complicated, increasing the risk of legislation failing to keep up with technology.

"Digital assets will make things incredibly efficient. So eventually your car will be represented by a digital token, your house will be represented by a digital token, you'll be able to do all sorts of things with that token. Digital portability will be important to that, but it is a long way off in regulatory terms," says Mr Buckley.

Next generation architecture

The challenges that emerging technologies present to data legislation also apply to data portability itself, as the need to be able to control and port data will become more significant as distributed-ledger technologies (DLT) continue to develop. Although still a nascent ecosystem, Web3 will be primarily built on these decentralised blockchains and "be orchestrated with tokens", according to an investor who has helped popularise the vision.[33]

Rather than being held on a centralised server owned by an entity, as is the case with the present Web2, data in Web3 would be stored in a DLT.[34] Although primarily known as the technology underpinning crypto-assets, blockchain has also been widely adopted in many different types of financial and technology applications.

Essentially, a blockchain stores data in blocks, which are chronologically connected and bound by cryptography. Once in the chain, the data can no longer be altered, as the chain can only be added to.[35] New tokens, generated through "mining", are used to incentivise entities to maintain and protect the integrity of the data stored.

In terms of data portability, this offers a new model where data can be shared across nodes, and data owners can grant or withdraw permission to access their data, reducing the role of platform owners in the storage, transmission and monetisation of their data.

Decentralised data

For some Web3 evangelists, like Mr Sena, the evolution of blockchain and its applications constitutes an opportunity to return the internet to its utopian democratic ideal, where information is innately interoperable.

[33] "What is Web 3?, Kevin Roose, *The New York Times*, https://www.nytimes.com/interactive/2022/03/18/technology/web3-definition-internet.html

[34] Blockchain & Distributed Ledger Technology, World Bank Brief, April 12th 2018, https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt

[35] What is Blockchain technology, IBM, https://www.ibm.com/au-en/topics/what-is-blockchain

"When Tim Berners Lee set out to create the internet, it was meant to be a platform of interoperable information," he says. "As big companies came around, they centralised the internet on their own servers, in their own networks. So the internet went from this open network where anyone can do anything into this network of walled gardens. In some ways, [Web3 is] just restoring the initial vision of the internet and returning it back to the people."

However, not all Web3 applications are beneficial to society or inherently democratic. Cryptocurrency's anonymising capabilities, for example, can be used to facilitate crime such as money laundering or terrorism. And although public blockchains such as Ethereum and Bitcoin are permissionless and decentralised, private or permissioned blockchains, like R3's Corda, Hyperledger and a blockchain for Central Banks from Ripple, allow only authorised users to access the data, meaning that not all data are necessarily available to all users. These private blockchains have fewer nodes than the public ones, which makes them faster and more energy efficient at the expense of decentralisation.

In reality, many hope that Web3 technology will revert the internet to its true, founding ethos. However, at the same time, the data portability products that are being built to support this are more often focused on improving the architecture that powers many businesses and services and diminishing the friction of the internet, as opposed to achieving its potential for greater democratisation.

In Australia, for example, where data portability in the banking sector is starting to roll out and is due to be expanded to telecommunications and energy, Mr Buckley says the efficiencies have been significant, even in small things like payment times. Describing data portability and the technology that enables it as "sewerage engineering for the modern economy", he says it not only provides "the pipes through which data flows", but also helps perform the hygiene function that keeps that data clean and reusable.

Alex Cordona, co-founder and COO of Codat, which builds integrated payments services for small businesses using its API, says that data portability also helps remove "document tennis". Using a loan application as an example, he says data portability enables credit paper applications to be pre-filled and effectively pre-approved, which reduces the costs of preparing the loan and its documentation "by about 75%".

And while this benefits consumers and small businesses, Mr Cordona says the financial institution itself also benefits, as it can then make better credit decisions, both at the point of application and throughout the life of the loan, because data portability provides it with constant, updated data on the performance of the business it is lending to. It also disproves concerns that the costs of data portability can be onerous, especially for smaller businesses.[36]

Portability models

Web3 technology and distributed shared ledger systems enable new ways of managing personal data, many of which are being trialled at present and all of which provide new opportunities for data portability.

Personal data vaults, for example, operate on the principle that data always remain the property of the data owner, who can allow data users to access these vaults. One company that already offers this service is the US start-up headed by Mr Chang, called Spruce. He says the aim of Spruce's data vaults is to let users control their

[36] Data Portability, Interoperability and Digital Platform Competition, https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf

data across the web and "get rid of the really bad principal-agent problems that we have with platforms".

"We think the best way to facilitate data portability is to move to a model where instead of users having to log into platforms, the platforms have to log into the user's data vaults, and the data vaults are wholly controlled by the user," explains Mr Chang.

In the data vault model, companies come to individuals asking for permission to use their data. Individuals can tailor data access and duration, and an API then accesses the data vault. Data owners gain, in principle, greater control over how their data are used and, with the right security protocols, are less vulnerable to data breaches.

Another means for managing data privacy and portability are data trusts, whereby people entrust their data to third-party intermediaries, also known as data stewards. These stewards interact with platforms on the data owners' behalf, ensuring proper consent and keeping them informed on what parts of their data are being used and how.

More sophisticated data trusts, like European-based Weople, offer an additional service of de-identifying personal data. Weople enables people to download an app and then activate a safe deposit box for data, which requests data from platforms including social media, Google, Apple, e-commerce purchases and store loyalty cards.[37] The app provides customers with a record of their data, which Weople then masks and anonymises to sell as part of data sets. Some of the profit is then returned to the data owner in the form of a digital currency.

Data trusts can be profit-driven companies or membership-based organisations like Weople, or not-for-profit organisations whose users choose to steward their data with them because of the social causes supported by the revenue generated from its use.

The market for the data that companies like Weople sell is growing, with governments and other organisations seeking legal access to large sets of data to train AI programmes to perform large-scale tasks with greater efficiency.[38] The Data Trust Initiative in the UK, for instance, is running pilot projects to explore how shared and aggregated data stewarded through data trusts can be used as inputs to AI and machine learning programmes. In turn, this could help to improve services in areas like civic amenity and public health.[39]

Decentralised databases offer another option, where data owners could be the stewards of their own data and supply different kinds of data to businesses with different conditions attached. In this case, a smart contract could exist on a blockchain, specifying how data can be accessed in exchange for some form of remuneration. This could remove the liability for data breaches for companies, but it places the onus of data security on the owners of the data themselves, rather than a third party, like with a data vault.

Mr Budish says there is no one ideal model, but that there are concerns that some of the portability models that are emerging may put business interests above those of the consumer. He says data portability tools need to be about finding a balance between giving people choice and control over their data, and providing privacy, protection and security to users. "Striking that right balance is not easy," he says.

Within this balance, data security is one of the

[37] See: https://weople.space/en/

[38] The future of data trusts and the global race to dominate AI, Bennett Institute for Public Policy, June 10th 2021, https://www.bennettinstitute.cam.ac.uk/blog/data-trusts1/

[39] See: https://datatrusts.uk/about

most contentious challenges. Ms Forbes says that although it is great to have "new entrants" to facilitate data portability, she would like to see a minimum-security threshold for them to operate.

"Having some baseline minimum expectations of who might have the resources or has the infrastructure in place to truly be able to secure and to deliver those compelling propositions seems quite reasonable to me to govern and protect the environment for users," she says.

Mr Swire says there are always risk/reward trade-offs, but that "effective authentication is absolutely necessary" for data portability, and that sensitive data like financial records and health data require particularly strong cybersecurity. He also notes that incumbent companies have an incentive to claim that there is a "terrible cybersecurity problem" and to occasionally use that as an excuse not to share data.

Ms Inge says as long as there are ways to address the risks, they shouldn't be a reason to give up on data portability. Mr Cordona agrees and says any level of cybersecurity is possible in practice. "The only problem is that the more secure the data is, the more expensive the cybersecurity costs are," he adds.

An emerging solution that can maintain data privacy while achieving effective authentication is zero knowledge proof (ZKP). First conceived in the 1980s, ZKP uses cryptography to allow information to be verified without the actual information being revealed.[40] It works well with blockchains, where information is bound sequentially and cannot be reverse solved.

ZKPs are used to verify transactions while maintaining confidentiality in some cryptocurrency exchanges and machine learning platforms. However, they also have strong potential as a portable digital identity solution, where identities can be authenticated online without people having to provide their personal details. This mitigates the risk of privacy being breached due to data hacks and theft.[41]

ZKPs can also be used to maintain data privacy by indicating that thresholds have been reached without disclosing actual numbers. A client applying for a loan could, for instance, show with a ZKP that they have qualified to borrow money without having to reveal the full details of their assets, income and liabilities.[42]

Regardless of the solution, many experts agree that it is only a matter of time until the technology evolves and these tools become mainstream, paving the way for full data portability and fundamental improvements in Web3 applications.

"Web3 as a term is evolving and getting figured out. But we can see the emergence of new architectures being pioneered, [which espouse] data portability and user sovereignty. It's really possible, when everyone has a digital key, or portability, to make digital statements and participate in an even playing field," says Mr Chang.

[40] What are Zero Knowledge Proofs, Lily May Newman, Wired, September 14th 2019, https://www.wired.com/story/zero-knowledge-proofs/

[41] How Does Zero Knowledge Proof Authentification Help Create a Portable Identity Solution, Dilip Kumar Patairya, Cointelegraph, October 14th 2022, https://cointelegraph.com/news/how-does-zero-knowledge-proof-authentication-help-create-a-portable-digital-identity-solution

[42] Can Zero Knowledge Proofs Enable Trust Within Financial Services? Steven McCann, InfoSys Consulting, November 4th 2022, https://www.infosysconsultinginsights.com/2022/11/04/can-zero-knowledge-proofs-enable-trust-within-financial-services/

The consumer perspective

While debate around the feasibility and challenges of data portability is necessary, the consumers who own the data in question are often forgotten. According to Economist Impact's global survey of 1,500 consumers, there is a need for more education about data portability and the legislative rights to protect individuals' online identities as well as considering future data portability options.

Technology companies also need to continue to focus on building more user-friendly data portability tools that are intuitive and secure. It's an issue that Ms Lange says Google has spent a lot of time considering. "I wish people would know more about [data portability tools]. I wish people would use them. I think that there's a fear in the industry that's unfounded," she says.

Trust and caution

One of the motivators to change is often fear, yet the survey results reveal a surprisingly large gap between a consumer's level of trust in

digital businesses and the actions or caution exercised in response. There is no correlation between the self-assessed measure of trust that consumers in the survey have in the digital businesses they interact with and the measures they take to mitigate their personal data security risk.

Instead, many consumers appear almost apathetic to data security issues and the level of trust more closely correlates with age, employment and gender. Consumers who are more trusting are generally younger, employed and have higher levels of education.

In comparison, caution is highly correlated with education levels. Those who take greater steps to protect their data are generally better educated and live outside of Europe.

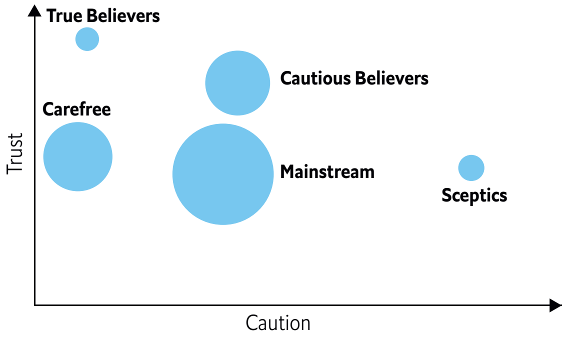
The survey respondents can be divided into five groups: the Mainstream, the Carefree, the Cautious Believers, the True Believers and the Sceptics.

Such division provides insight into who is more likely to be early adopters of data portability and a decentralised internet and who will require more time and greater education to adapt.

"It's often just not knowing the technical term for what can be a great feature that a consumer finds on a platform. There's probably a [lack of recognition] that these tools exist and that they are data portability tools, per se," explains Mr Budish. "People don't necessarily have to know that they're using a data portability tool in order to benefit from it."

For example, Europeans in the sample are less trusting than people from other regions, but they are also less cautious, while women are less trusting than men, but not more cautious. Although counterintuitive, this has important implications for digital businesses and the way they introduce data portability to different types of consumers and for consumer awareness of data portability.

Figure 1: Trust and caution



Source: Economist Impact.

The largest group, the Mainstream, for example, are likely to be open to data portability tools, although their use of these is likely to lag tech-savvy early adopters. The Carefree, in comparison, show lower caution despite not being more trusting, and tend to be slightly older and less educated. This group has a higher share of retirees and homemakers, with more respondents located in Europe and less in Latin America than other clusters. This group is unlikely to readily use data portability, as they lack the trust and caution that act as drivers of adoption.

The third group to emerge, the Cautious Believers, have high trust in digital business providers, and take some caution to protect their data. This group also has a higher share of younger people and the highest share of Millennials (born between 1980 and 1995[43]) of all the segments, meaning they are more digitally savvy than the Mainstream or Carefree. Their high trust levels are likely to motivate them to embrace data portability.

[43] Millennials, baby boomers or Gen Z: Which one are you and what does it mean? The BBC, https://www.bbc.co.uk/bitesize/articles/zf8j92p

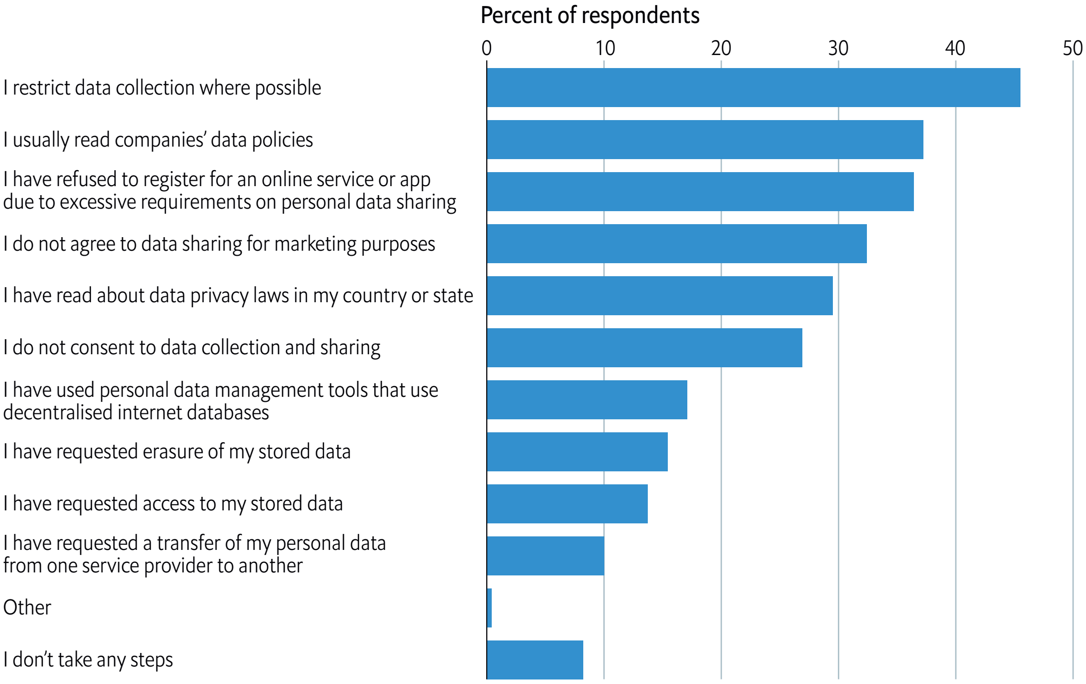
The last two clusters, the True Believers and the Sceptics, are the most extreme of the cohorts. True Believers have high levels of trust and low levels of caution. This cohort has more women and finance professionals than other groups and the highest share of Gen Z (born approximately after 1997). This group is likely to be among the early adopters of data portability, given their high trust and low caution. Considering that they show less concern about the choice of data management platform, it is reasonable to expect that the adoption will be driven by an immediate need to switch platforms or services, rather than by the need to safeguard and control their data.

In comparison, the Sceptics show very high levels of caution, despite not being, on average, less trusting, and are the oldest group, with a skew towards Gen X (born between 1966 and 1980). This segment has higher levels of education but the lowest average levels of income and more self-employed and IT professionals. These people take, on average, the most steps to protect their data and put the most thought into the tools they use for this purpose. This group is likely to be educated on data portability and demanding in terms of features and tools that are offered to them.

Data awareness

The internet has become an inherent part of people's lives. The way consumers now interact with apps, online tools and media signals a dramatic shift in technology utilisation, paving the way for greater adoption of distributed technology systems. Over 80% of the survey respondents use social media or instant messaging platforms daily. In addition, more than half (59%) streamed video or audio content

Figure 2: What steps have you taken to control the personal data that companies collect on you? (Multiple selections allowed)



Source: Economist Impact.

at least once a day in the past month, while 39% had played video games. Over a third (37%) had also made financial transactions online, while only 7% had made a crypto-asset transaction.

The ubiquity of social media and users' evolving preferences in this highly competitive landscape, together with the growing consumption of online content and the expanding range of online services, demonstrate a need for new, flexible and secure ways of managing consumers' data and digital identities.

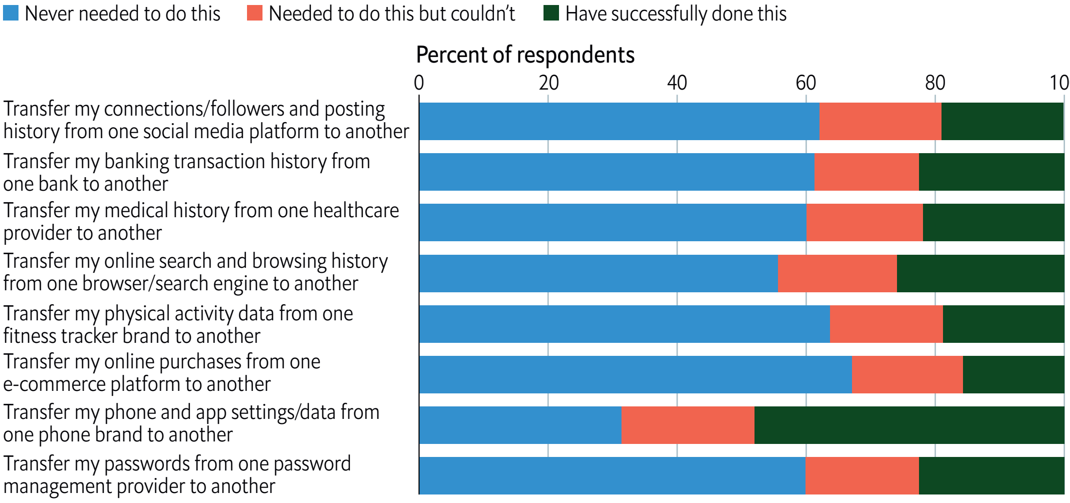
However, despite the frequent interaction with platforms and services that collect and make use of personal data, consumers are generally not aware of how the data are used—and few make an effort to control or safeguard it. Just over a third (37%) say they usually read companies' data policies, only 32% say they do not agree to data sharing for marketing purposes and 30% claim to have read about data privacy laws in their country or state. This underscores a need for much greater education around data use and portability.

And although almost half (46%) of consumer respondents say they restrict data collection where possible, this percentage differs among generations: Baby Boomers were more likely (55%) to report such restriction than Gen X (48%), Millennials (43%) and Gen Z (38%). This suggests that people who have grown up with the internet don't place the same premium on privacy as those who have not.

Most respondents are also passively agreeing to data collection on platforms they interact with; only 27% do not consent to their data being collected and shared. And while 17% had used personal data management tools with decentralised internet databases, only 10% of respondents had requested a transfer of data from one service provider to another, showing that data portability is not a key concern for most consumers.

This low rate of personal data portability may also come from a needs basis. When asked whether they had transferred a range of personal data, over 60% had never felt the need, a connection that Ms Lange has observed. "People don't think about it until they want to do a specific thing related to data transfer. And then,

Figure 3: Have you ever been in any of the following situations where you wanted to or tried to transfer your data from one service provider to another?



Source: Economist Impact.

when they do, that's when they would explore their options," she says.

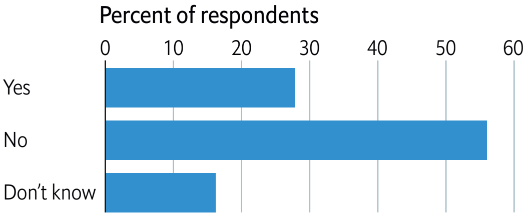
This statistic contradicts another observation that 69% of respondents had, at some point, a need to transfer data from one mobile device to another that is a different brand (70% of them did so successfully). This suggests that some data portability applications have already become part of our lives and don't register in users' consciousness as such.

Overall, 84% of respondents had a need, at some point, to transfer data from one service provider to another. Nearly half (43%) were unsuccessful.

Transferring phone app settings and data from one phone brand to another was the most common, with 48% of respondents having done this successfully, while a quarter (26%) had transferred their online search and browsing history from one search engine to another. However, in an indication that the companies that provide these services need to become more user-friendly, 21% of consumers had needed to port their phone data but failed, while 19% had also failed to port their browser history.

It reinforces the fact that awareness of the technology that facilitates data portability is low. Just 28% of respondents said they had stored or managed their personal data on a platform that uses a decentralised internet database, such as blockchain, which conflicts with the 17% of respondents in figure 2 who said they had used personalised data management tools with decentralised internet databases.

Figure 4: Do you store and manage any of your personal data using a platform that uses a decentralised internet database, such as blockchain?



Source: Economist Impact.

"The literacy and education around this is quite low, unfortunately," says Mr Chang. "There are ways to talk about the benefits of data portability, in real terms, without diving into the technical ... because not everyone should become a privacy expert. I think it's a little insolent to assume that everyone should just learn privacy and data as well as data experts."

It is also an area where regulation can help. "The GDPR is actually good on this basis in the focus and insistence on simple language and placing the onus back on to data controllers and processes," Mr Cordona says. "Being very explicit about those things means that it is hard to be accused of misuse at some point later down the line."

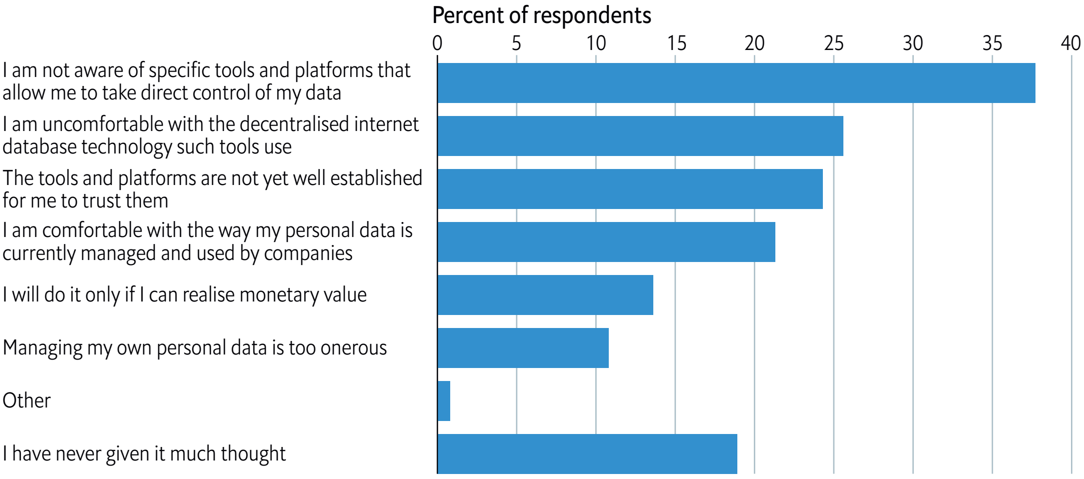
Further highlighting the technological confusion among consumers, 56% said they had not stored or managed their personal data on a platform that uses a decentralised internet database, yet 16% of respondents said they didn't know if they had, a much higher rate of uncertainty than usually seen in surveys.

This lack of awareness of data portability is placed in even greater context when the 56% of consumers who said they don't store and manage any of their personal data using a platform that uses a decentralised internet database were subsequently asked why they don't do this. Well over a third (38%) of this group said they are not aware of any specific tools and platforms that allow them to take direct control of their data, in addition to the 16% who indicated "don't know" in the original question.

Data trust

From the survey results, consumers' trust in technology is heavily influenced by the type of organisation they deal with online. When asked which types of organisations they trust to use

Figure 5: What is the reason why you do not store and manage your personal data on a platform that uses decentralised databases? (Multiple selections allowed)

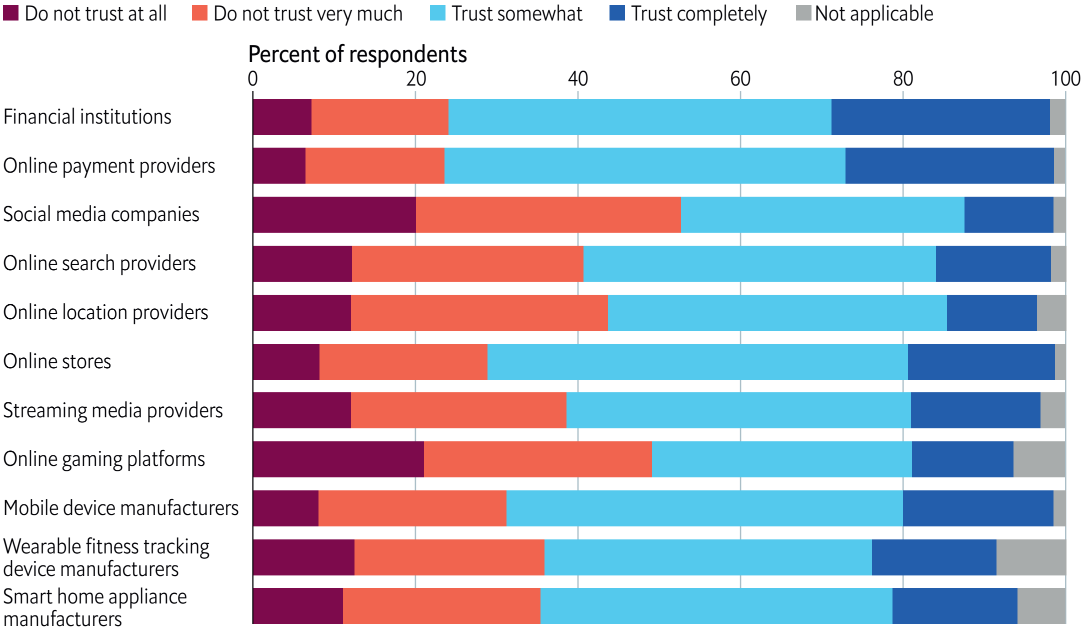


Source: Economist Impact.

personal data only for their benefit, finance, retail and mobile phone companies are clear leaders. Online payment providers (75% trust completely or somewhat) and financial institutions (74%) are the most trusted, followed by online stores (70%) and mobile device manufacturers (67%).

At the other end of the spectrum, social media

Figure 6: How much do you trust the following types of organisations to use your personal data for your benefit only?



Source: Economist Impact.

companies are the least trusted, with 53% of respondents saying they have little or no trust the companies will only use the data they are provided with for the owner's benefit, followed by online gaming platforms (49% do not trust at all or not very much) and online location providers (44%).

With social media being the most popular type of online activity respondents participate in, this points to what has been referred to as the 'privacy paradox', whereby people don't trust the platforms they give their personal data to, but continue to do so nonetheless.[44] One likely theory for this is that the risk/reward assessment of potentially losing privacy is outweighed by the perceived rewards of curating and displaying identities and interacting with other people,[45] while users may also value the instantaneousness of connection over their privacy.[46]

Mistrust of social media platforms is stronger among older respondents, with 70% of Baby Boomers, 54% of Gen X, 48% Millennials and 43% Gen Z mistrusting them either completely or somewhat. While trust in other platforms and services was more evenly distributed, Millennials overall were the most trusting. Asia-Pacific respondents are also the most trusting when it comes to financial institutions and online payment providers, and Americans the least.

Europeans also have a higher level of mistrust in social media companies (60%) than those from the Americas (50%) and Asia-Pacific (48%). Yet they are least likely to read data collection policies (33%) compared with the Americas (42%) and Asia Pacific (37%). It is possible that Europeans put greater trust in their regulators and the GDPR to hold companies to account. This may also reflect the fact that European respondents tended to be older, more often retired, and used online services, on average, less than those from other regions.

Shared perspectives

The privacy paradox, which many academics believe is based on a risk/reward sentiment, also applies to the types of data that consumers are comfortable sharing, and the types of data they would consider making available to other corporations in exchange for a payment or a service they provide, which is often referred to as data monetisation.[47]

Mr Chang baulks at the idea: "Why would you want to have the same company that makes money by selling you advertising also host all your most personal information?" But sharing personal information about their identity, likes and dislikes, and location is something the world's 4.7 billion social media users do every time they log in.[48]

This is also reflected in the survey responses. Half of respondents would be willing to share their data with a third-party organisation if that company needed it to provide a service, 20% said they would only share their data for a financial reward and 12% said they would gladly always share their data. Only 17% of people said they would not share their personal data so a company can provide a service.

As figure 7 indicates, consumers are more willing to share their data for crime prevention and law enforcement, for scientific research, and to help a company improve the functioning of its

[44] Explaining the privacy paradox, a systematic review of literature investigating privacy attitude and behavior, N. Gerber, P. Gerber and M. Volkamer, *Computers & security*, August 2018;77:226-61, https://www.sciencedirect.com/science/article/pii/S0167404818303031

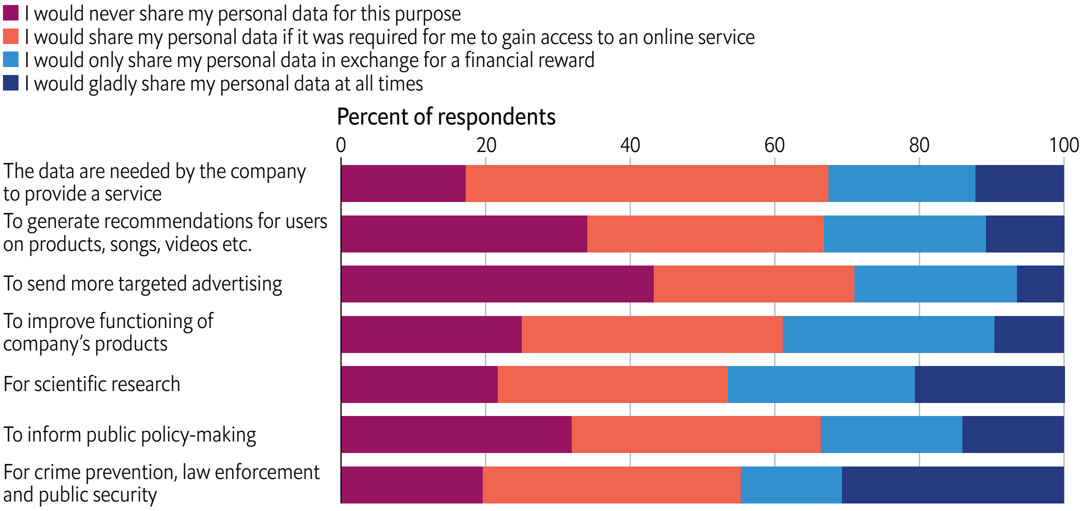
[45] Why We're So Hypocritical About Online Privacy, Tomas Chamorro-Premuzic and Nathalie Nahai, Harvard Business Review, May 1st 2017, https://hbr.org/2017/05/why-were-so-hypocritical-about-online-privacy

[46] Online privacy concerns and privacy management: A meta-analytical review. Baruh L., Secinti E., Cemalcilar Z., *Journal of Communication*. February 1st 2017;67(1):26-53, https://onlinelibrary.wiley.com/doi/abs/10.1111/jcom.12276

[47] Data Monetization, Gartner Glossary, Gartner, https://www.gartner.com/en/information-technology/glossary/data-monetization

[48] Digital 2022: July Global Statshot Report, DATAREPORTAL, July 21st 2022, https://datareportal.com/reports/digital-2022-july-global-statshot

Figure 7: For each of the following use cases, please indicate your willingness to share your personal data with third party organisations.



Source: Economist Impact.

products. They are less comfortable with sharing data for advertising and content algorithms, but well over half of all consumers are still willing to share data for these purposes, especially if they can gain access to a service or receive payment.

This willingness to improve product functioning is important, as consumers may be more open to education outreach regarding data portability and Web3. It could also be critical to the development of new, more user-friendly tools that are designed around consumers rather than the technicalities of a data portability function itself.

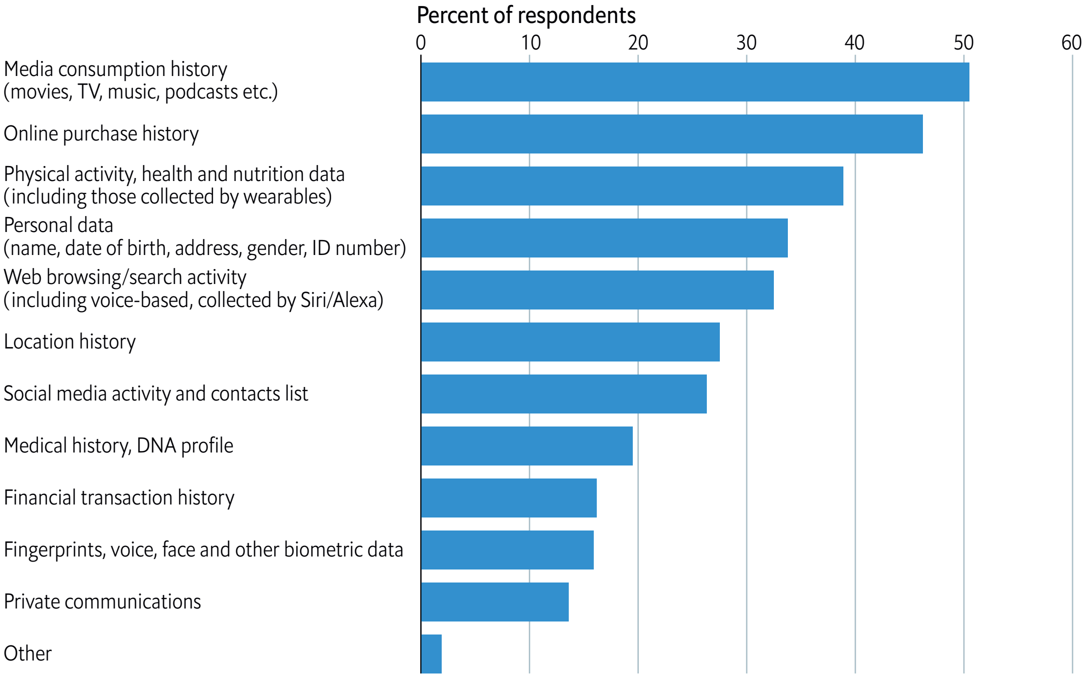
Personal data may not be tangible, but it is recyclable, meaning data owners can trade the same information in return for service provision again and again. This could make data portability tools like data vaults or tokenised identities valuable, as they could make trading this information less time consuming and potentially rewarding. The 20-30% of respondents who claim they would only share their data in exchange for a financial reward could also be a strong attractor for those attempting to set up data intermediaries like Weople or Web3-based data trusts.

Consumer comfort with sharing data also depends on the types of data they are being asked to reveal. So while 51% are happy to share media consumption history in exchange for a payment or service, 47% are happy to provide their online purchasing history and 39% their health and nutrition data, just 16% are happy to share their financial transaction history or biometric data and 14% their private communications.

The extent to which consumers are prepared to share their data varies across sectors. Younger people (Gen Z and Millennials) are almost twice as likely (21%) to be happy to share their financial transaction histories, for instance, as Gen X and Baby Boomers (12%), suggesting their greater adoption of online banking, as were those in Asia (23%) compared with Europe (12%) and the Americas (14%).

This highlights the need for data portability tools that are designed around different types of data, with highly personal data like healthcare likely to

Figure 8: Which types of data would you consider making available to other corporations in exchange for a payment or a service they provide? (Multiple selections allowed)



Source: Economist Impact.

need very different models than entertainment data, for example.

Mr Sena is aware of the complexities this creates for the balance between data portability and security and says different types of data have very different security needs, which means there won't be a 'one-size-fits-all' data portability system or infrastructure that consumers will be able to access in the future. "But it does feel like there will be pieces and components that interoperate nicely," he says.

Google's Ms Lange agrees. "I do think there needs to be different portability tools for different data types. Health and financial data are different from photos and email, in the sense that losing it, or losing control of it, carries much higher risks," she says.

However, the openness to sharing data depending on the outcome is also a positive, according to Mr Sena. He says while building apps on a decentralised platform is easy, getting the data to populate these apps and generate the machine learning needed for development is much harder. If more consumers are willing to share their data, this could drop the barrier to entry for new developers, and result in a better Web3. "More creativity allows developers to take their ideas to market faster and experiment. All of these things are net positives," he says.

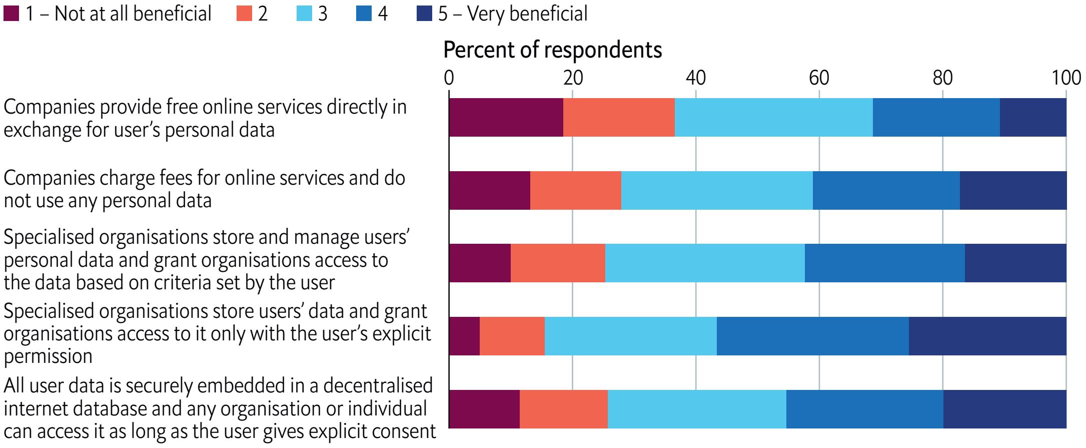
Maintaining control

Awareness of data portability tools and data privacy may not be high. However, the need for portability and security expressed by consumers, and the sophistication that many consumers display when ranking the data they would trade, show that such tools may have a healthy potential user base. But this would only come about if some of the inherent challenges to data portability could be overcome.

More than a third of consumers (38%) aren't aware of tools and platforms that allow them to take direct control of their data, while 26% are uncomfortable with the Web3 technologies these tools use, and 24% think the technology is insufficiently established to be trusted. Building awareness (including a distinction between Web3 apps and crypto-assets) and developing new tools are both essential for businesses keen to prosper in this market.

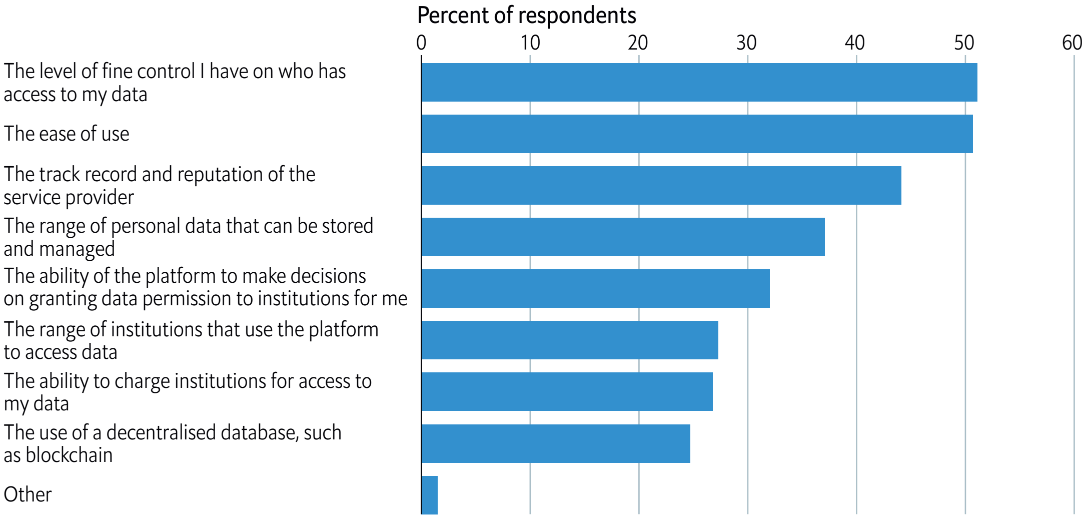
When asked which ways of managing personal data would be most beneficial to society, 57% of

Figure 9: Which of the following ways of managing personal data do you think would be most beneficial for society?



Source: Economist Impact.

Figure 10: What criteria are important to you when considering a personal data management platform, such as blockchain? (Multiple selections allowed)



Source: Economist Impact.

respondents chose a data intermediary model, where specialised organisations store users' data and grant organisations access to it only with the user's explicit permission.

The second most popular model was where data are securely embedded in a decentralised internet database that any organisation or individual can access, if the user gives explicit consent.

This issue of consent is vital, and it is the most important criterion to consumers when considering a personal data management platform such as blockchain.

The preference for explicit consent implies a desire for control that doesn't currently exist, paving the way for a range of new data portability models. But these will need to be intuitive, as ease of use is the second most important feature consumers would like to see in a personal data management platform. Many consumers are still unaware of or indifferent to the advantages of data portability. But if portability can be provided in a user-friendly way that gives control back to the user, it could help hasten the tipping point for the adoption of such technologies and accelerate the path towards a digital future.

Conclusion

Data portability is likely to become more viable and important with the increasing meshing of our online and offline selves. Together with data privacy, it is a key data right for individuals. However, data portability faces roadblocks that currently prevent greater acceptance and availability.

Even when there has been the will to try and overcome these hurdles, the technology to achieve the necessary interoperability for effective data portability remains beset with challenges. Current regulation such as the GDPR has done much to articulate what data portability and the right to it are. Even though it has effectively encouraged big tech to establish data portability projects, like the DTP, it has not substantially increased its level of implementation and availability for consumers. As a result, consumer awareness of data portability remains low. Small to medium-sized businesses and those not in the technology space are also ill-prepared for the required changes.

Arguably, the main issues with data portability are technological rather than regulatory. However, Web3 technologies such as distributed shared ledgers and ZKPs are likely to revolutionise the relationships between data users and owners and how data are ported between them. Regulators will have to tread carefully between facilitating these advances while keeping people's data safe.

Developers also need to be focused on developing data portability tools that provide adequate security and grow the range and sophistication of tools to match different types of data. Only when easy-to-use consumer products that help people manage data privacy and portability are available, will awareness and interest take off.

Key learnings

- **Data portability is a right.** Current data portability legislation has succeeded in articulating the right to data portability, but in most cases has done little to activate it. Legislators will have to keep up with emerging technologies and tread the fine line between enabling innovation and protecting data owners. They also need to help prepare businesses of all sizes to adapt to a future where data portability is the norm.
- **Security is a key challenge.** One of the key problems with data portability is maintaining adequate data security when it is transferred and/or accessed. Security needs also differ depending on the data being ported. Data portability tools will need to become more

sophisticated to accommodate this. Until the security of highly personal data can be guaranteed, true data portability will be at risk.

- **Consumers need to be educated.** Consumer awareness of data portability and its potential benefits is low. This will likely only change when people feel the need to port their data or discover that Web3 data portability tools reduce the friction and enhance the security of their online experiences. Education programmes that help grow understanding would benefit not just consumers but the technology companies eventually offering those tools.

- **More consumer research is needed.** More user experience research is required to help guide the development of new data portability tools. Research is also required into what will be needed to turn consumers on to emerging data portability tools, and how they are most likely to use these tools.

- **Increased investment and innovation are needed.** Data portability is not a one-size-fits-all solution. Consumers' entertainment preferences, for instance, will have different portability parameters compared with sensitive data such as those concerning health and finances. This means that investment and innovation in different types of data portability tools will be necessary.

- **Businesses and consumers need to be prepared for the tipping point.** Web3 applications such as data vaults have the capacity to revolutionise data portability but the tipping point for their uptake is likely sometime in the future and will be contingent upon technological advances in computational power. However, once viable, the change will be swift and any disruption will be smoother if governments, businesses and consumers are prepared.

Methodology and demographics

Economist Impact commissioned an online survey of 1,500 respondents, which was conducted in September and October 2022. It consisted of ten content, and seven demographic questions.

The survey targeted a broad demographic of people who use online services daily. Of the 1,500 respondents, 500 were from each region—Asia-Pacific, Europe and Africa, and the Americas.

Age and location

Location	Baby-Boomers (1946-64)	Generation X (1965-80)	Millennials (1981-96)	Generation Z (1997-2004)	TOTAL
Africa	15	38	37	45	135
Asia Pacific	37	134	168	161	500
Europe	120	134	64	47	365
Latin America	28	131	118	46	323
North America	46	67	50	14	177
Total	246	504	437	313	1,500

Gender

Male	Female
721	778

Education

Primary	Secondary	Tertiary vocational	College or university	Post-graduate degree
30	380	249	623	215

Employment status

Employed	Self-employed	Unemployed	Student	Homemaker	Retired	Other
896	208	98	94	57	130	14

Statistical analysis

For the purpose of the analysis, we created two variables from the dataset: trust and caution. The first is a measure of self-assessed trust in a variety of digital business sectors. Caution refers to how many measures respondents have taken to mitigate personal data security risk.

The analysis employed two statistical techniques - hierarchical clustering and linear regression. Clustering identified five distinct groups of respondents based on the similarity of their trust and caution responses. We further analysed the clusters through exploratory data analysis on different demographics such as age, region, gender, and employment status of the respondents. We also made use of other content questions such as the frequency of use of different online services or the willingness to share personal data online, to examine the characteristics of the five clusters. We used tests of significance to gauge statistical differences in the average trust and caution levels of different groups with respect to the average levels for the sample.

To substantiate our findings from the cluster analysis, we used linear regression, which is a controlled analysis that quantifies how demographic factors contribute to each of the two variables of interest, trust and caution. We then based our insights on the values of the statistically significant regression coefficients.

While every effort has been taken to verify the accuracy of this information, Economist Impact cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report. The findings and views expressed in the report do not necessarily reflect the views of the sponsor.

ECONOMIST IMPACT

LONDON

The Adelphi, 1-11 John Adam
Street, London, WC2N 6HT
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
Email: london@economist.com

GENEVA

Rue de l’Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@economist.com

NEW YORK

750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@economist.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@economist.com

HONG KONG

1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@economist.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@economist.com