Digital Future Society

Privacy-first:

a new business model for the digital era

A programme of

GOBIERNO DE ESPAÑA

VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

MOBILE WORLD CAPITAL BARCELONA

About Digital Future Society

Digital Future Society is a non-profit transnational initiative that engages policymakers, civil society organisations, academic experts and entrepreneurs from around the world to explore, experiment and explain how technologies can be designed, used and governed in ways that create the conditions for a more inclusive and equitable society.

Our aim is to help policymakers identify, understand and prioritise key challenges and opportunities now and in the next ten years under key themes including public innovation, digital trust and equitable growth.

Visit digitalfuturesociety.com to learn more

A programme of

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es

MOBILE WORLD CAPITAL™ BARCELONA

Published
March 2020.

Disclaimer
The information and views set out in this report do not necessarily reflect the official opinion of Mobile World Capital Foundation. The Foundation does not guarantee the accuracy of the data included in this report. Neither the Foundation nor any person acting on the Foundation's behalf may be held responsible for the use which may be made of the information contained herein.

Contents

Executive Summary

Once a by-product of digital transformation, data has become the fuel that drives modern technological development. Although data analytics bring new possibilities for governments, businesses, and citizens, there is growing concern that models based on the extraction of data by any means necessary have become the norm.

The proliferation of digital platforms and connected devices has contributed to increasingly sophisticated methods of data extraction, especially when it comes to personal data. 2018 was the year the term "surveillance capitalism" was coined to express the invasive nature of such business practices, the threat they pose to individual privacy, and even democracy as we know it.

Meanwhile, governments worldwide face the difficult task of balancing data flows to encourage economic growth with protecting citizens' privacy. Conscious of this delicate balance, the United Nations has called for a "society-wide conversation, based on informed consent, about the boundaries and norms for such uses of digital technology and AI."[1]

Information laws such as the General Data Protection Regulation (GDPR) are only starting to take effect. Nonetheless, legal experts and privacy advocates recognise that regulation can only go so far in preserving privacy in real terms. Regulation combined with the so-called "techlash" — the growing mistrust in tech companies — has sparked the emergence of a new set of businesses. The latter prioritise privacy, trust and transparency as core values over profit and growth. This report refers to them as "privacy-first". Still niche, these emerging business models challenge the data-extractive paradigm that currently drives the digital economy.

Even though there is a market need for privacy-first solutions, these businesses face a myriad of barriers. Their main competitors are platform businesses that control the market and benefit from network effects. Few options for funding and slow growth trajectories pose additional challenges for privacy-first businesses to reap the potential of their value proposition.

Governments can play an important role in incentivising their growth especially because these businesses are an exception in the tech industry. In addition to shedding light on their emergence, along with the opportunities and challenges of privacy-first business models, this report serves as a call to action for policymakers to think beyond regulation and engage with private sector actors that are building a digital economy based on trust, transparency and privacy.

The report draws on the conclusions of the Digital Future Society Think Tank working group on digital trust and security. Written for policymakers, this report paints a clearer picture of these innovative new business models and analyses four cases of existing privacy-first businesses that are profitable. It concludes with three proposals that policymakers can implement to specifically address the challenges and leverage existing opportunities, while creating new ones.

[1] Digitalcooperation.org. 2019

Glossary

Data broker

A data broker is any kind of entity that collects, aggregates and sells individuals' personal data, derivatives, and inferences from disparate public and private sources.[2]

Data extraction

The process of collecting data from different sources such as the online activity of internet users. For companies with a data monetisation business model, this is a necessary first step to later analyse, process and extract profit from this information.

Decentralised cloud

A network of multiple connected devices in which anonymised data and information are stored. This model is an alternative to large cloud data storage companies, which potentially involve several risks (control by private companies, threat of massive leaks, vulnerable infrastructure, etc.) to the security and privacy of the data.

Encryption

Encryption is a method to convert a message or information into code in order to conceal its true meaning. Decrypting the content requires a key or password. This is a standard technique used to increase the security of any kind of digital communication.

General Data Protection Regulation

The General Data Protection Regulation replaced the Data Protection Directive in 2018. The aim of the GDPR is to provide one set of data protection rules for all European Union member states and the European Economic Area (EEA).[3]

[2] Nytimes.com 2019

[3] Iapp.org 2019

Network effect

In economics, the network effect refers to a phenomenon whereby a larger number of users or customers increases the value of a good or service. Issues such as the quality or utility of the product, its price or brand awareness define the scope of this effect. Among online service platforms or networks such as social media, it is usually a crucial success factor.

Open-source

If software is open-source, its source code belongs to the public domain. The term also represents a more participatory and democratic business approach than software with a private license. Open-source software can be modified and shared with any recipient and for any purpose. The distribution of this code must be totally free, non-discriminatory and technologically neutral.[4]

Platform economy

The platform economy encompasses all digital platforms that put users in contact with the services offered by one or more companies. This definition includes platforms that facilitate commercial transactions, such as Amazon or Uber, but also the technological frameworks that allow for the development of digital businesses.

Privacy by Design

A concept first outlined in a framework in the mid-1990s by former Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian. The term refers to the idea that data processing procedures should already integrate data protection when a digital product or service is first created.

Surveillance capitalism

Coined by social psychologist Shoshana Zuboff, the term refers to a market in which large technology companies collect users' behavioural data for commercial purposes. This can have significant — and sometimes detrimental — implications for the control and surveillance of society, both by public and private actors.[5]

Unicorn

In the venture capital (VC) industry, a unicorn is a start-up valued at more than 1 billion USD. This requires exponential growth in terms of users as well as the ability to generate revenue quickly. Among the most well-known unicorns are Airbnb, Uber, Ant Financial and SpaceX.

Vendor lock-in

A business model strategy used by some companies to restrict the customer's right to switch to an alternative technology or product provided by a different vendor. Changing providers typically involves a high cost in time and money. This practice, which limits market competition, has spread in recent years to sectors such as data storage services.[6]

Zebra

In the start-up ecosystem, zebras symbolise a business model and a set of values that directly contrast with those represented by unicorns. The term originates from a movement led by several women entrepreneurs with the aim of "creating alternatives" to the start-up culture status quo.[7] The foundational principles of these companies include sustainable growth, a non-discriminatory culture and an ethical approach to business.

[4] Opensource.org 2019

[5] Couldry 2016

[6] Schacklett 2018

[7] Brandel et al 2017

Introduction

The data economy and its discontents

The International Data Corporation estimates that global revenues from big data and business analytics applications will reach 274.3 billion EUR by 2022.[8] Although data-driven applications offer endless possibilities for businesses, there is a growing concern on behalf of policymakers, academics and civil society on the potential invasiveness of data extraction when it comes to personal data.

Given the nature of online data collection, certain types of companies are better designed and therefore more inclined to benefit from its opportunities. These businesses are platform services that have reached significant scale and benefit from network effects. Part of this competitive advantage results from the ability to build large datasets.[9]

From there, they improve their offering based on data analytics and insights which further entrenches their positions as market leaders. Platform services like Google, Facebook, and Amazon capitalise on the value created from data as they retain it through the whole chain. In this ongoing quest to maintain market dominance and amass ever larger sets of data, digital platforms have created an ecosystem that supports data as a new form of economic capital, the accumulation and circulation of which must be constant.[10]

Data encompasses information generated by machines and humans alike. However, certain data monetisation models run the risk of viewing users as free sources of data. The user as “raw material” is a recurrent theme among disruptive digital business models. Not only do these business models predict consumer behaviour, but they seek to maximise profit by using data to influence and modify user behaviour.

Social psychologist Shoshana Zuboff has termed this model "surveillance capitalism.” In a system where our every move feeds predictions of what we will do now and in the future, according to Zuboff, society risks being divided into two groups: those who monitor and those monitored, creating a new form of "inherently anti-democratic" social inequality.[11]

[8] International Data Corporation 2019

[9] GSMA 2018

[10] Sadowski 2019

[11] Naughton 2019

Growing privacy concerns

Although online privacy advocates have been present ever since the commercialisation of the internet, they are now more visible than ever. Data leaks and breaches have heightened public awareness on the culture of surveillance. A growing awareness of the role of personal data in digital business and the potential erosion of individual privacy has shifted privacy concerns that once were characteristic of hacker culture to mainstream culture. This shift is evident in an October 2018 statement by Apple CEO Tim Cook:

> **Our own information, from the everyday to the deeply personal, is being weaponised against us with military efficiency. (…) Every day, billions of dollars change hands and countless decisions are made on the basis of our likes and dislikes, our friends and families, our relationships and conversations, our wishes and fears, our hopes and dreams. (…) These threads of data, each one harmless enough on its own, are carefully assembled, synthesised, traded, and sold. Taken to its extreme, this process creates an enduring digital profile, and lets companies know you better than you may know yourself.**[12]

This shift in consumer awareness opens a window of opportunity for privacy-focused technologies. A set of businesses with a shared ethos to protect users' data is emerging and has made a conscious decision to forgo potential revenues derived from the personal data economy. In doing this, these companies renounce a type of model that is highly profitable within the current data economy and the growing trend of data extractivism.

About this report

The purpose of this report is to help policymakers identify business models with privacy as their core value and to explore how they can incentivise their growth. This report refers to these business models as privacy-first: businesses that are non-extractive since they do not monetise personal data.

The content of this report draws on the work produced by a group of six international experts who came together for two and a half days in Barcelona in September 2019, as well as on additional desk research.

The report begins with an overview of the origin of data-extractive business models and continues with a brief explanation of the digital tools that make up the privacy ecosystem, which sets the scene for the report's focus: privacy-first business models.

Through the analysis of four profitable privacy-first companies, the report discusses their challenges and opportunities in competing with market leaders that profit from user data in exchange for "free" services. These privacy-first businesses are defined through a set of guidelines, available in the annex, which can serve as a standalone tool for policymakers to identify privacy-first companies.

The focus of the final section is based on the working group's ideation. It discusses possible ways in which policymakers can use these guidelines to support value-driven businesses. In addition, the three initiatives proposed in this report respond to the opportunities and challenges encountered by these privacy-first companies.

Audience

This report is primarily written for policymakers, with the aim to offer insights to anyone working within government who must write or implement rules governing frameworks and regulations that intersect with technology, and especially those who are participating in public innovation and public procurement services. This report could be equally beneficial for institutions advocating for equitable data governance. Additionally, it might be useful in regions with low levels of data regulation, as these ideas could create meaningful impact in evolving stronger data governance policies.

Scope

Why focus on privacy-first business models?

Privacy-first businesses position themselves in opposition to the extractive data economy or "surveillance capitalism" model. This report analyses the business models of these companies as well as their data handling practices. These businesses can be described to be living models of Privacy by Design (PbD) as stipulated in the GDPR regulation.

The report acknowledges the limitations of both regulation and PbD principles. Critics have pointed out the vagueness of both, highlighting the need to define methodologies to bridge the gap from theory to practice. There is much ground to cover since society has yet to see regulation's impact on businesses and citizens. By limiting the scope of this report to business models that have successfully prioritised privacy over profit, we aim to shed light on how abstract data governance concepts are being transformed into practice.

[12] Asher Hamilton 2018

What kind of data are we talking about?

This report uses the definition of personal data as described in the GDPR: any public or private information that can be traced back or used to identify a person, directly or indirectly, including cultural, physiological, and social attributes (see Appendix II).

Given the complexity of data governance,[13] an in-depth analysis of the limitations of regulation on a global scale falls outside the scope of this report. However, the GDPR is used as a starting point to facilitate discussion. By using this landmark data regulation as a reference, the report argues that even the GDPR, which provides stronger data protection for citizens than other regulations, has its limitations. Considering that privacy-first businesses selected for the report are based in Europe and the United States, privacy-first businesses can have a greater impact in markets of countries with weaker data protection laws.

As there is extensive literature on data governance, data supply chains, and privacy regulation, this report seeks to add to the ongoing conversation by shifting the focus from regulation to incentives. While this report recognises the value and limitations of regulation, the incentives proposed at the end of this report are designed to compliment the regulatory actions already taking place around the world.

[13] See Digital Future Society report Towards better data governance for all 2019

1

Data-driven business models in context

How did we get here?

The data monetisation model has its origins in the early stages of Google. Until then, data was used to improve the quality of products, especially in terms of user experience. Used this way, data was an asset for companies like Apple, whose revenue depended on hardware. A search engine like Google, however, saw little return on investment even as they provided a better search experience for users. Pressured to find ways to retain investors and survive as a company, Google found a way to generate revenue with the surplus of behavioural data it had amassed on its users: targeted advertising.[14]

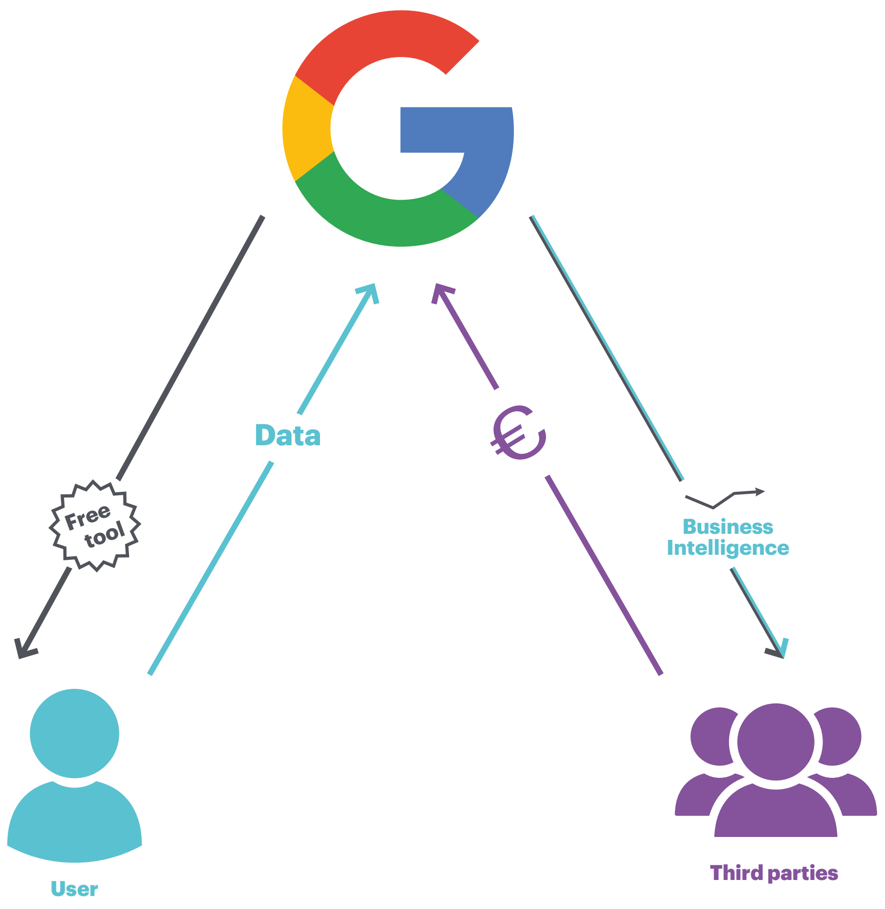


Figure 1: A breakdown of the user data monetisation business model. Google search collects all types of data about its users: search terms, references displayed, locations, languages, etc. It then offers third parties ad targeting and demand forecasting services.

Image source: Adapted from Business Model Toolbox.

Data source: Zuboff 2019

[14] Zuboff 2019

Since then, data monetisation has evolved from Google's first use case and expanded to other sectors. Parallel technological advancements have propelled the capacity for data collection and driven the economic potential of data monetisation models. The accumulation of data along with the rise of mobile, smart devices, IoT and social media have contributed to more sophisticated business models.

Four major trends drive the growth of the data monetisation business model

1 **Rise of platforms**	Advancements in machine learning and computational power backed by large scale infrastructure allows for the accumulation of observed data.
2 **Increase in mobile adoption**	Mobiles and smartphone apps create a new way to obtain location and behavioural data through tracking.
	It is expected that by 2025, 71% of the world's population will be mobile subscribers. [15]
3 **New ways of capturing data with IoT**	The proliferation of smart devices like wearables mean more types of data will be commercially traded.
4 **Popularity of social media**	Inferred user profiles, through personal data have opened opportunities for business, academia, government, and civil society.

Figure 2: Major trends driving the growth of the data monetisation business model.

Image source: Digital Future Society

Data sources: Digital Future Society, GSMA

[15] GSMA 2018

Extracting value from data

There are two main revenue streams that businesses can pursue when monetising data. The deciding factor is whether the company has the capacity to perform in-house data analysis. Those who do not have the infrastructure or technical know-how can license raw data access to clients. Data licensing was Twitter's strategy.[16]

Companies that possess the internal infrastructure and technical skills in data science can offer a variety of revenue-generating services, such as targeted advertising, demand forecasting or dynamic pricing services. Amazon marketplace, for instance, uses data obtained from purchases, product reviews and locations. Based on this data, it offers third parties consulting services, demand estimates and trends. One inference, for example, could be where a vendor should build their next warehouse.[17]

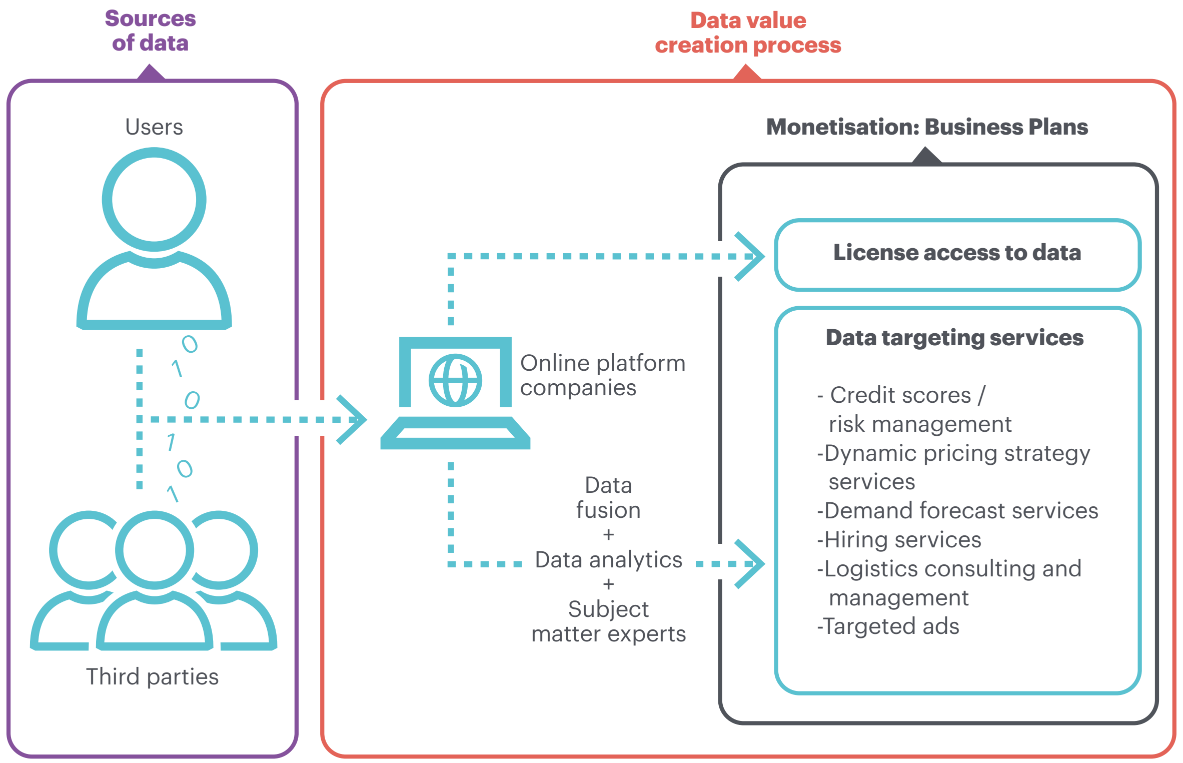

Sources of data
Data value creation process
Users
Third parties
Online platform companies
Data fusion + Data analytics + Subject matter experts
Monetisation: Business Plans
License access to data
Data targeting services
- Credit scores / risk management
-Dynamic pricing strategy services
-Demand forecast services
-Hiring services
-Logistics consulting and management
-Targeted ads

Figure 3: The data value chain.

Image source: Adapted from Ly et al. 2019.

[16] Ly et al. 2019

[17] Ibid.

The risks we face

According to privacy expert Ann Cavoukian, the risk involved in the data extraction business model is dual: not only do these practices jeopardise the privacy rights of consumers vulnerable to data leaks and cyberattacks, but the company's own integrity is at risk.[18]

Such concerns have reached a supranational level. A recent report by the United Nations highlights the urgency of rebuilding trust and guaranteeing the right to privacy, threatened by new possibilities for the surveillance, tracking and monitoring of citizens.[19] To do so, it proposes a "society-wide conversation, based on informed consent, about the boundaries and norms for such uses of digital technology and AI."[20]

In addition to putting privacy at risk, data-extractive business models pose a threat to market competition and innovation. The growth of digital platforms and the driving force of data has led to the concentration of influence and power in the hands of a few companies.[21] In the absence of national and global regulations, market leaders end up dictating the rules on data availability and use. This reality directly affects the competitiveness of other, smaller players in the data economy, such as SMEs.[22]

Data governance and its limitations

At the time of writing, over 100 countries have data protection laws or regulations in effect.[23] While some business leaders and policymakers fear that innovation will be stymied by the introduction of these laws, this pushback has begun to fade following the Cambridge Analytica scandal. Nonetheless, the conversation is still divided between those who are aware of the privacy risks inherent in data monetisation models and those who seek to implement policies that facilitate global data flows. The latter could possibly stimulate privacy-invasive business models – making privacy-first business models more important for a digital future grounded in trust and transparency.[24]

Regarding data protection regulations, governments around the world have faced a range of challenges and opportunities in developing policies that safeguard individual privacy and civil liberties in digital contexts. One of the most relevant (due to the magnitude of the market it affects) is the GDPR of the European Union.

Compulsory since May 2018, this law has tightened control over data processing practices, under the threat of fines for companies that fail to comply. The GDPR also expands the jurisdiction of prior legislation in that even foreign companies that process EU residents' data must comply.

[18] Jones 2018

[19] Digitalcooperation.org 2019

[20] Ibid.

[21] Faravelon et al. 2015

[22] Un.org 2019

[23] Unctad.org 2019

[24] Sugiyama 2019

However, using regulation as the sole policy lever to counter personal data misuse poses several limitations:

1 Intervention after the fact

Legislation such as the GDPR sets a series of rules that companies must implement when they collect and process data. At the same time, companies must be able to demonstrate compliance with regulatory standards.[25] Only when a company fails to comply with the rules do the authorities intervene through penalties. This *ex-post* regulatory approach does not guarantee privacy-respecting data use, since the final responsibility lies with the company to comply and the user to intervene if they would like to regain ownership of their data.

2 Non-personal data could have the same impact as personal data

Another limitation is how personal data is defined, which differs depending on the legal jurisdiction, and whether regulating personal data collection can actually mitigate the practice of targeted or personalised advertising. Under the current GDPR regulation, for instance, profiles can be built by tracking users' online activity, inferring without explicitly collecting any data on beliefs, sexual orientation, race or ethnicity.[26] The ambiguity of existing regulations allows companies to use proxy attributes: inferred characteristics based on likes or online behaviour. With profiles built on non-personal data, companies can capitalise on these sensitive inferences.

3 Anonymisation of personal data is not always effective

One of the measures promoted and recommended by the GDPR is data anonymisation. According to the regulation, personal data is not considered personal when anonymised. However, recent studies reveal how it is impossible for researchers to fully protect real identities in datasets. In most cases, anonymised data can be cross-referenced with information in other databases to identify the original source of the data.[27] This limitation sheds light on the challenges and complexities of data governance.

[25] GDPR 2019

[26] Wachter 2019

[27] Ohm 2010

4 Between theory and practice

The GDPR has been critiqued for its vagueness and lack of specificity regarding how each article should be applied.[28] For some experts, the regulation is a step forward regarding Privacy by Design principles, however it does fall short in providing concrete guidelines for companies to comply.[29] One example that illustrates this gap is consent.

Consent is one of the most common methods companies use to obtain personal data partly because it is one of the easiest legal grounds to satisfy.[30] While the GDPR clarifies that consent should be freely given and users must understand and accept how their data will be used, this requires ensuring that the consent forms are in plain language (no legal jargon), dynamic (allowing consent to be withdrawn), and granular (allowing many different forms of consent).[31]

The efficacy of consent mechanisms is hotly debated among experts.[32] While instruments of consent were conceived to enable users to make informed decisions about their personal data, legal experts doubt their practicality and whether this responsibility should be placed on users in the first place as it is difficult to consider all possible ramifications when giving consent.[33]

Looking beyond regulation

These are just some of the limitations that demonstrate how challenging it is for policymakers to keep pace with technology companies in the context of data governance. Although data protection regulation may seem like the only mechanism to curb data extractivism, there are other ways governments can actively disincentivise personal data monetisation models across the data economy.

Economist Mariana Mazzucato argues that governments have a crucial role in creating markets, not only fixing them. "The point is not to prescribe specific technologies," she explains, "but to provide directions of change around which bottom-up solutions can then experiment."[34] In Mazzucato's vision of the entrepreneurial state, governments act as catalysts for technological opportunities by creating "a network of willing agents (not necessarily 'winning' agents) that are keen to seize this opportunity through public-private partnerships."[35]

[28] Downes 2019

[29] European Union Agency for Network and Information Security 2018

[30] GDPR.eu 2019

[31] Ibid.

[32] Herrle and Hirsh 2019

[33] Ibid.

[34] Mazzucato 2015

[35] Mazzucato 2017

A new type of digital business: the privacy-first model

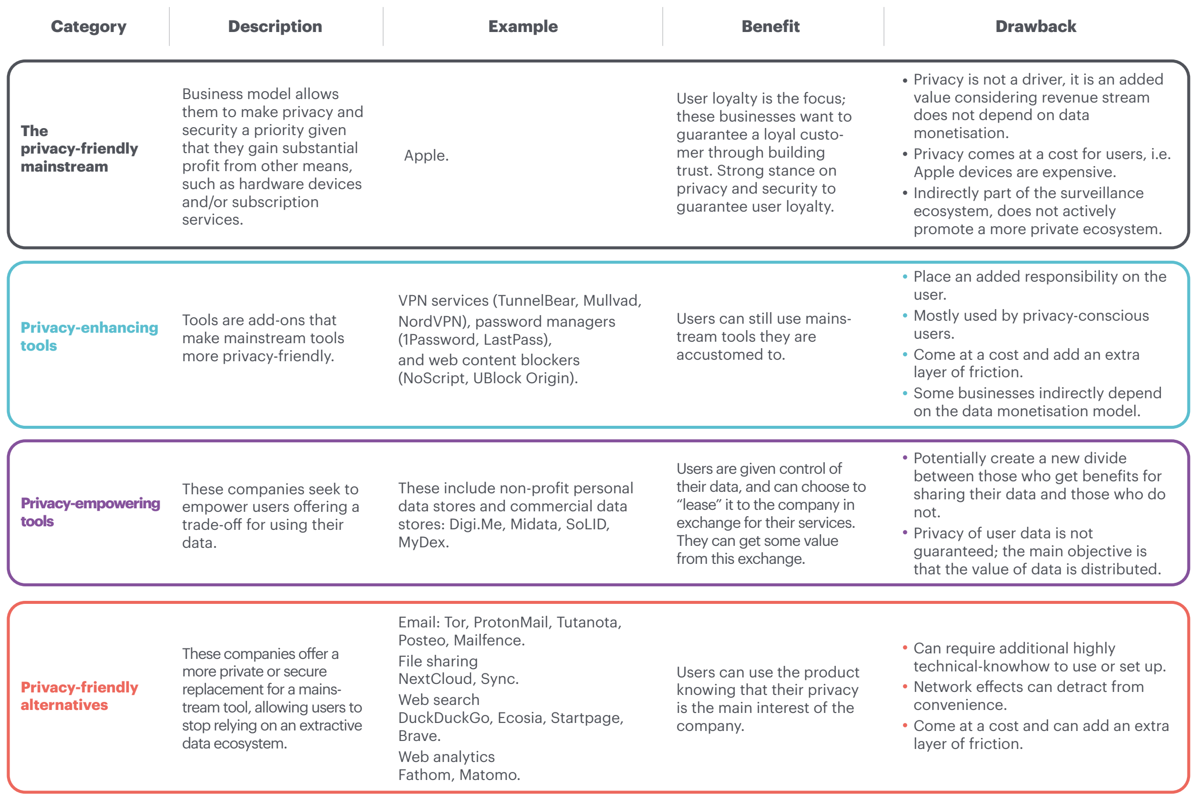
In the context of the current data economy trading in extractivism and surveillance, these "willing agents" are businesses that are already responding to a market need for stronger data privacy.

Given that privacy-first businesses are not the only ones that offer solutions to data extractivism, the table below provides an overview of other players in this emerging ecosystem, as well as the benefits and drawbacks for their users.

Juxtaposing these businesses provides a clearer picture of how privacy-first businesses position themselves in the broader digital market.

Ecosystem of privacy-respecting businesses and tools

The table below illustrates different players in the digital privacy ecosystem. They may share the same objective and challenges, however, the main difference is that privacy-first businesses seek to replace a mainstream tool.



Category	Description	Example	Benefit	Drawback
The privacy-friendly mainstream	Business model allows them to make privacy and security a priority given that they gain substantial profit from other means, such as hardware devices and/or subscription services.	Apple.	User loyalty is the focus; these businesses want to guarantee a loyal customer through building trust. Strong stance on privacy and security to guarantee user loyalty.	• Privacy is not a driver, it is an added value considering revenue stream does not depend on data monetisation. • Privacy comes at a cost for users, i.e. Apple devices are expensive. • Indirectly part of the surveillance ecosystem, does not actively promote a more private ecosystem.
Privacy-enhancing tools	Tools are add-ons that make mainstream tools more privacy-friendly.	VPN services (TunnelBear, Mullvad, NordVPN), password managers (1Password, LastPass), and web content blockers (NoScript, UBlock Origin).	Users can still use mainstream tools they are accustomed to.	• Place an added responsibility on the user. • Mostly used by privacy-conscious users. • Come at a cost and add an extra layer of friction. • Some businesses indirectly depend on the data monetisation model.
Privacy-empowering tools	These companies seek to empower users offering a trade-off for using their data.	These include non-profit personal data stores and commercial data stores: Digi.Me, Midata, SoLID, MyDex.	Users are given control of their data, and can choose to "lease" it to the company in exchange for their services. They can get some value from this exchange.	• Potentially create a new divide between those who get benefits for sharing their data and those who do not. • Privacy of user data is not guaranteed; the main objective is that the value of data is distributed.
Privacy-friendly alternatives	These companies offer a more private or secure replacement for a mainstream tool, allowing users to stop relying on an extractive data ecosystem.	Email: Tor, ProtonMail, Tutanota, Posteo, Mailfence. File sharing NextCloud, Sync. Web search DuckDuckGo, Ecosia, Startpage, Brave. Web analytics Fathom, Matomo.	Users can use the product knowing that their privacy is the main interest of the company.	• Can require additional highly technical-knowhow to use or set up. • Network effects can detract from convenience. • Come at a cost and can add an extra layer of friction.

Figure 4: Digital privacy ecosystem overview.
Image source: Digital Future Society

[36] Etherington 2019

2

Case studies

Privacy-first in practice

Privacy-friendly alternatives are companies that seek to replace a mainstream tool, such as a search engine or email provider, with a privacy-conscious alternative. Privacy-first businesses are unique because they do not put the responsibility of data protection on the user. They are designed in such a way that data protection is inherent and functional from the beginning. The personal data they collect is none to minimal and contrasts with the data extractive business model by handling data transparently and securely.

To address the main question of how policymakers can support and incentivise privacy-first business models, this report analyses four case studies of profitable privacy-first businesses: DuckDuckGo, ProtonMail, Nextcloud, and Matomo.[37] Not only do these companies comply with existing regulation, but they go beyond to ensure trust through other mechanisms, such as auditability, accountability, and verifiability. All four recognise the user as the main beneficiary and share a similar long-term strategy: to build a more private internet.

Most importantly, this report identifies these alternatives to emphasise the role of privacy-first business models in changing the exploitative nature of the current data economy, given that data extractive models can still practice invasive profiling and behavioural tracking even under current privacy regulations.

[37] See Annex III of this report for an extended list of privacy-first businesses.

DuckDuckGo

DuckDuckGo is a search engine that does not track users' behaviour or collect their personal data. Founded in 2008 by Gabriel Weinberg, DuckDuckGo is a well-known privacy-first alternative to mainstream search engines. With a staff of 86, its headquarters are in a small town in the United States. DuckDuckGo currently processes an average of 1.3 billion monthly searches, having experienced exponential growth in recent years.[38] However, its market share of 0.4% is still miniscule compared to dominant search engines.[39]

Mission and vision

According to the company, "too many people believe that you simply can't expect privacy on the internet. We disagree and have made it our mission to set a new standard of trust online."

Commitment to privacy, security and transparency

DuckDuckGo did not begin as a privacy-protecting search engine. Its founder originally conceived the business to elevate the user experience of online search by improving results, reducing clutter, and eliminating spam. Weinberg identified privacy as an increasingly common concern among users and adopted it as a personal cause, betting that it would become a growing concern among internet users in the long term.[40]

In terms of value proposition, the main difference between DuckDuckGo and other search engines is that it does not share search terms with third parties. Although it collects keywords, it does not associate them with users or identify people who have used them. Unlike most websites, DuckDuckGo does not store user identification data such as IP addresses.[41]

On the other hand, the mobile app and browser extension offer a system to measure privacy (Privacy Grade) that shows how much a site can be trusted.[42] Features include forcing users to use encrypted connections when available and stopping advertisers from tracking users on the sites they visit.

Part of the DuckDuckGo architecture is built from Free and Open Source Software (FOSS).[43] Additionally, the company is increasing its commitment to collaborative software development through its GitHub site,[44] focusing on its Instant Answers, static sites and community platform, among other projects.

[38] Lomas 2018

[39] StatCounter 2019

[40] Weinberg 2011

[41] DuckDuckGo 2019

[42] Ibid.

[43] Ibid.

[44] Github 2019

Finally, almost every year since its foundation, DuckDuckGo donates to organisations that contribute to raising the standards of online trust. In 9 years, the total volume of donations has reached 1.9 million USD. This pursuit to rebuild trust in digital business is reinforced through its own blog Spreadprivacy.com, which includes privacy tips for users, and other educational material to spread online privacy awareness.

Business model

All DuckDuckGo tools (search engine, applications and browser extension) are free to use. The company generates revenue in two ways. The first is through contextual advertising: the ads on the search page are based on the search terms themselves and not enhanced by any stored data, as is the case with major search engines. These ads, distributed through the Yahoo! Network, appear as sponsored links at the top of the page.

Its second revenue stream is generated through an affiliate program with e-commerce platforms Amazon and eBay. If a user visits these sites while using DuckDuckGo and makes a purchase, the company receives a small commission.

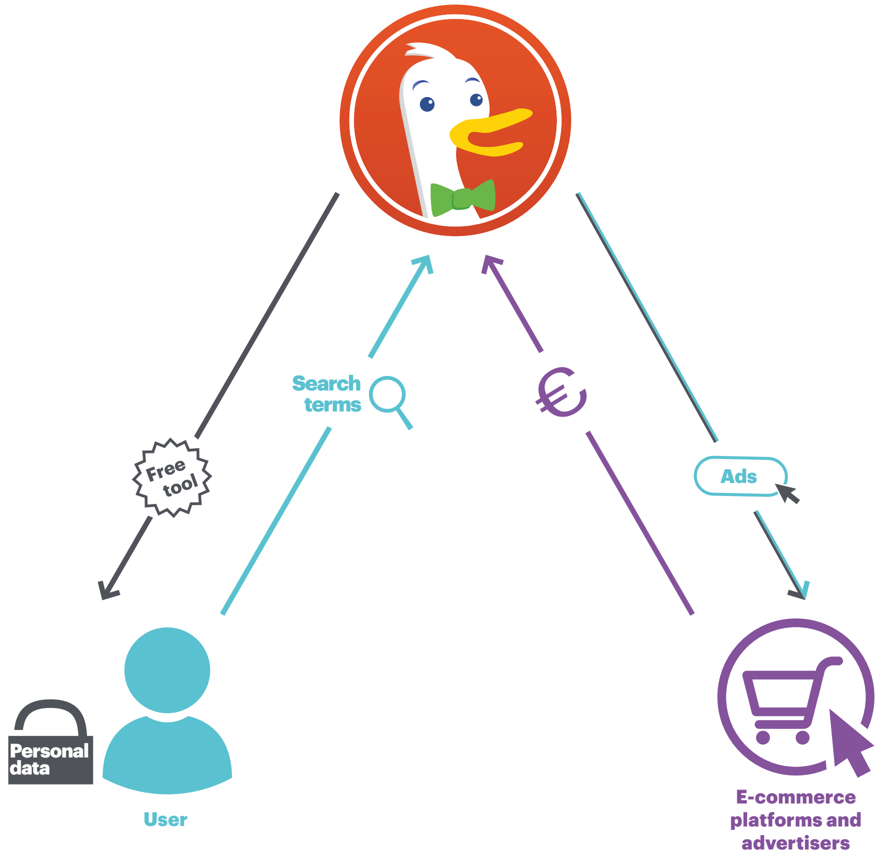


Figure 5: The DuckDuckGo business model.
Image source: Adapted from Business Model Toolbox.
Data source: DuckDuckGo 2019

Funding

DuckDuckGo is not Weinberg's first project. After graduating from MIT, Weinberg started an educational software company.[45] He later launched Names Database, a social network that was acquired by Classmates.com in 2006 for 10 million USD.[46]

DuckDuckGo was self-funded until 2011. That year, Union Square Ventures injected 3 million USD into the project, and in 2018 the venture capital arm of Canadian pension fund Omers invested another 10 million USD.[47]

The company experienced significant growth a few years after its foundation. In 2012, DuckDuckGo already accounted for an average of 1.5 million searches per day. In 2014, Apple included it as one of the default search engines available for its Safari browser, and Mozilla did the same for Firefox. In 2019, even its direct competitor Google started adding DuckDuckGo as a search engine available for Chrome. In November 2019, DuckDuckGo hit a new peak in searches in a single day: 50.9 million.

Key takeaways

- DuckDuckGo proves that a free search engine can generate revenue without extracting user data with contextualised advertising as a non-invasive alternative.
- DuckDuckGo's long-term strategy is aligned with its company values as well as the market. Its development of other privacy-protecting tools is an indicator of its choice to pursue sustainable growth.
- The company's founder, Weinberg, is a serial entrepreneur whose previous experience raising capital gave him an advantage when presenting DuckDuckGo to venture capital firms, who bet on Weinberg's track record.[48]
- Although the company's main selling point is privacy, it works to deliver a browsing experience with accurate searches, less clutter and minimal spam.
- DuckDuckGo's advocacy work for privacy highlights the interdependence of privacy-first business models and the need for a privacy-respecting ecosystem that offers users a trustworthy internet where their personal data is safe.

[45] Chan 2019

[46] Sec.gov 2006

[47] Lomas 2018

[48] Burnham 2011

ProtonMail

ProtonMail was founded in 2014 at the European Organisation for Nuclear Research (CERN) research facility by Andy Yen, Jason Stockman and Wei Sun. With over 10 million users, ProtonMail's core objective is to protect and secure users' data through encrypted email. In contrast to the data-extractive ad revenue business model, ProtonMail seeks to transform email services by offering one that prioritises data protection. In 2018, ProtonMail teamed up with Mozilla to develop Proton VPN, a trustworthy and free virtual private network service with more than 1 million users.

Mission and vision

"We're building an internet that protects privacy, starting with email."

The ProtonMail team claims to share the vision and challenge of "protecting civil liberties online." To this end, its objective is to create an accessible and easy-to-use email tool for as many people as possible.[49] In the long term, the company seeks to develop additional privacy-first tools including a calendar, storage, and document editor.

Commitment to privacy, security and transparency

ProtonMail secures privacy by encrypting messages in the user's web browser before it reaches ProtonMail servers. They do this by generating a pair of keys on the user's computer. As ProtonMail does not hold the password nor keys for decryption, they cannot access user messages.

Apart from securing end-to-end encryption, the mail service does not collect users' IP addresses nor does it store users' encrypted data on a cloud. It uses a managed server in Switzerland (in a bunker 1000 meters under the Swiss alps). The creators chose the location because Switzerland has the strictest privacy laws globally and remains outside of US and EU jurisdictions.

ProtonMail slowly started making parts of its software packages open-source and plans on continuing to do so as it grows. By making the code and cryptography available for inspection, it reinforces transparency and auditability.[50] ProtonMail's commitment to transparency goes beyond the software, since the company statutes, employees and financing are publicly

[49] ProtonMail 2019

[50] ProtonMail 2015

documented. Their communication is transparent and evidence-based, and their work is vetted by third parties through external security audits and peer reviews, which are also published.

As part of its communication strategy, ProtonMail plays an active role in raising awareness and advocating for privacy rights. Some examples include creating GDPR.eu as a resource for small businesses on GDPR compliance, speaking at a UN conference on fighting terrorism while protecting human rights, working with Reporters Without Borders, and publicly opposing unregulated surveillance using facial recognition technology.[51]

Business model

The company claims that it does not show ads or make money by abusing users' privacy.[52] ProtonMail has a tiered pricing model. Its free service offers 500 MB of storage with a limit of 150 messages per day. For more storage, email addresses, messages and support, users can choose between three different packages offering more features. ProtonMail's revenue is used to support all accounts (including free subscribers) as well as technical support, research and development.

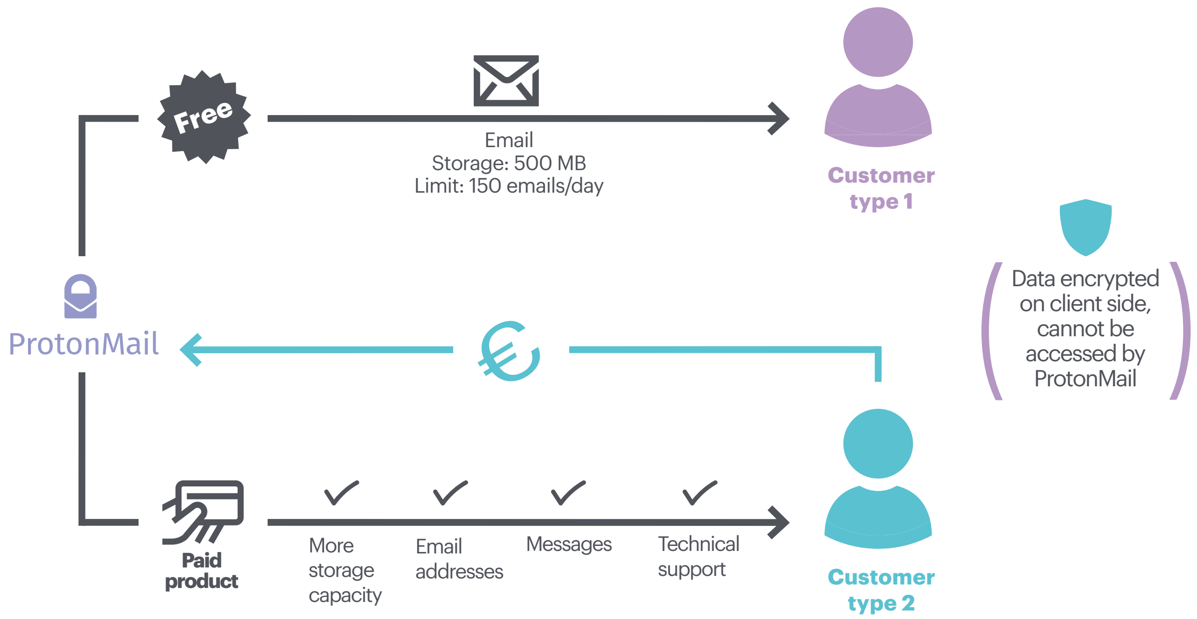


Figure 6: The ProtonMail business model.
Image source: Adapted from Business Model Toolbox.
Data source: ProtonMail 2019

[51] ProtonMail 2015

[52] Ibid.

Funding

ProtonMail started with an Indiegogo crowdfunding campaign in 2014 that raised 500,000 EUR. Its main stakeholder is the privacy-conscious community. In its commitment to protect user privacy, the company initially refused to accept investor funding.[53] In 2014, founder Yen said "the reason we have to be bootstrapped is because if we take our money from something like Google Ventures, there goes our credibility. By being in this market we have to fund ourselves."[54]

ProtonMail's main obstacle was finding private funding that aligned with company values.[55] In 2015, they received 2 million USD from US-based firm CRV (early investors in Twitter, Zendesk and Yammer) and the Fondation Genevoise pour l'Innovation Technologique (FONGIT), a non-profit foundation backed by the Swiss government.[56] In early 2019, ProtonMail was awarded 2 million EUR from the European Commission's Horizon 2020 programme to further develop the Proton ecosystem. According to the company, this partnership not only signifies "a meaningful amount of funding, but also a powerful ally in the tough battles to come."[57]

Key takeaways

- In order to prove that a business model is not based on data extraction, communication is key. ProtonMail is transparent and thorough when it comes to explaining how they protect user data.
- The CERN research facility and community played an important role in the inception of ProtonMail; the community provided technical know-how as well as product testing and validation.
- Swiss privacy laws and institutional backing provided a favourable environment for the creation of a privacy-first email service.
- Finding the right investment partners was key for ProtonMail to maintain its value-driven mandate.
- By aligning interests with European institutions, such as FONGIT and Horizon 2020, ProtonMail acquired the funding to develop further privacy-respecting applications.
- A tiered pricing model can be a useful intermediate alternative — between "freemium" and a full subscription model — for expanding the customer base while generating enough revenue to ensure financial sustainability.

[53] ProtonMail 2019

[54] Slade 2014

[55] Ibid.

[56] Sawers 2018

[57] Yen 2015

Nextcloud

Founded by Frank Karlitschek and a team of open-source engineers, Nextcloud is an open-source suite of services that provides an alternative model to centralised cloud services. Karlitschek started the project in 2016 after leaving OwnCloud, a company he had founded six years earlier but left due to diverging strategies.[58]

Nextcloud software allows individuals and businesses to self-host and manage their data. In addition to storage, Nextcloud offers:

- File sync and share which gives users access to files and allows them to work and share on documents with their teammates.
- A messaging platform that allows teams to screenshare or have meetings, all while data is stored locally on the server.
- Groupware: Integrates productivity features like calendar, contacts and mail.

Nextcloud estimates they have about 25 million users over 300,000 servers.[69]

Mission and vision

 "We develop software for decentralised and federalised clouds as an alternative to centralised cloud services."

Nextcloud enables the user to take control of their data when using its tools. In the long term, it hopes to be a part of a privacy-first ecosystem where various cloud services can provide a viable alternative to centralised, proprietary solutions.

Commitment to privacy, security and transparency

Nextcloud software is designed so that customers can build on the service to run on their own server or device. It allows users to take total control of data storage and can be integrated in the monitoring and logging tools used by the company. The software works with some of the most popular authentication mechanisms and protocols on the market.[60]

Nextcloud itself complies with data privacy and protection since they do not collect nor access any user data. They have, however, designed the product so that their customers can readily comply with the GDPR.

Privacy and transparency are the core values behind the product. As full control of data is guaranteed because it is self-hosted, Nextcloud is also open-source, meaning anyone can verify the absence of "backdoors" in the software. There is no vendor lock-in since users can run the software independently from Nextcloud with other service providers. As an open-source project, Nextcloud has a large volunteer community; over 2,000 people contribute code to the project.

Business model

The company is built on an open-source business model.[61] Nextcloud offers a freemium version with additional features depending on clients' needs. If clients do not have the technical expertise or resources to run the software, they can subscribe and access technical support from Nextcloud. Additional features include support, consulting, and integration with Outlook or Collabora's open-source office suite.

Nextcloud's growth strategy relies on slow, sustainable and organic growth. The company, which currently has 50 employees, turned profitable in 2017. Customers range from individuals to SMEs to large organisations, as well as third parties that run cloud services and offer Nextcloud as a product. Notable clients include the French and German national governments.

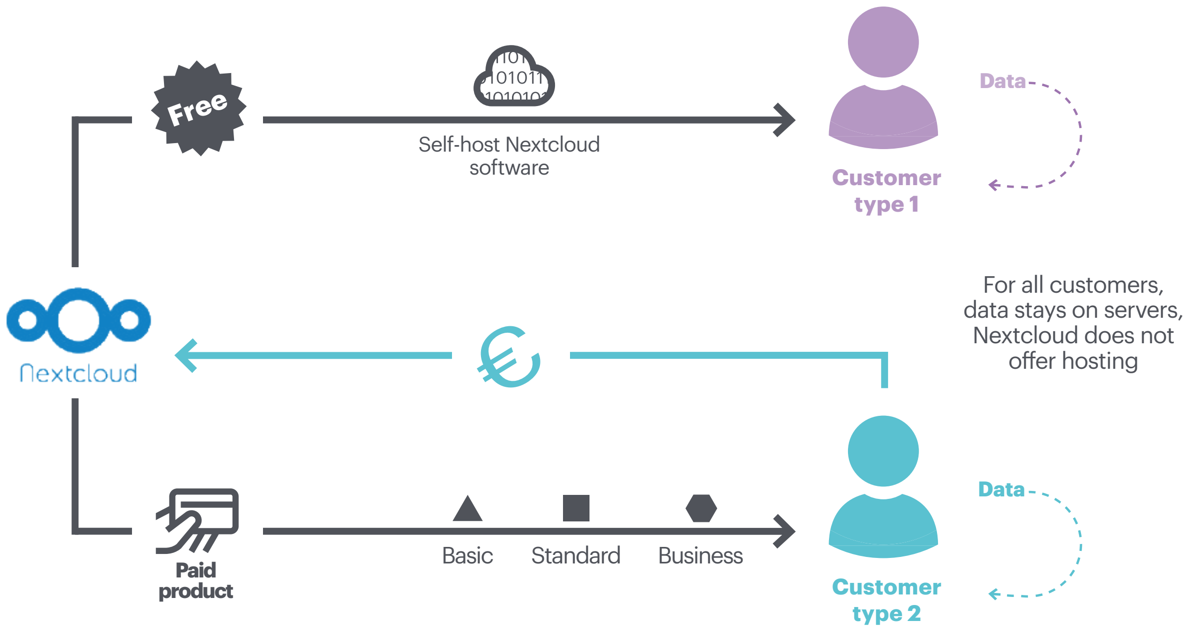

Free
Self-host Nextcloud software
Customer type 1
Data
For all customers, data stays on servers, Nextcloud does not offer hosting
Nextcloud
Paid product
Basic
Standard
Business
Customer type 2
Data

Figure 7: The Nextcloud business model.
Image source: Adapted from Business Model Toolbox.
Data source: Nextcloud 2019

[58] Yen 2019

[59] Karlitschek 2016

[60] Poortvilet 2019

[61] Nextcloud 2019

Funding

Nextcloud is employee-funded. Founder Frank Karlitschek eschewed venture capital given that his previous venture, Owncloud, was subject to specific conditions that opposed his value-driven vision for the company.[62]

Key takeaways

- Nextcloud offers a solution to both individuals and companies seeking to take ownership of their data.
- Governments and companies that are concerned over the growing concentration and centralisation of data have demonstrated interest in enterprise solutions offered by Nextcloud.
- Nextcloud is interoperable, meaning users can easily integrate it with other systems unlike the proprietary tools of its competitors.
- Community plays an important role in Nextcloud's business model, since open-source engineers contribute to coding and employees help fund the venture.
- The open-source business model promotes transparency and innovation but also requires extra effort on behalf of management to maintain the delicate balance between all stakeholders.

[62] Bhartiya 2016

Matomo (Innocraft)

Matomo is an open-source web analytics tool that allows companies to collect data through their website for decision-making purposes. The company behind it is Innocraft. Matomo software has its roots in Piwik, founded in 2007 by Matthieu Aubry, to fill the need for a privacy-conscious alternative to Google Analytics. It is used in over 200 countries and on one million websites.[63]

Mission and vision

Innocraft aims to position Matomo as the number one open-source analytics platform. The company actively participates in a larger movement to decentralise the internet.

Commitment to privacy, security and transparency

Innocraft's focus is to empower individuals and businesses to take control of their data. Most users host their analytics tool on their own servers. Therefore, the company cannot access any of their clients' data, reinforcing Matomo's Privacy by Design. Additionally, the software gives website owners more control over which pieces of data to track, helping them comply with GDPR regulation, in order to ensure that visitor behaviour is not shared with advertising companies. Matomo automatically anonymises visitors IPs and deletes old visitor logs.[64]

Innocraft asks for the collaboration of its user community to find security problems in its software.[65] It also has a reward system for those who find relevant security bugs and offers advice to users that want to improve their software's security.

[63] Matomo 2019

[64] Ibid.

[65] Ibid.

Business model

Innocraft has an open-source business model. Users can host Matomo Analytics on-premise and pay for support or additional features. If clients do not have any technical expertise, they can pay to store their data on the cloud. Innocraft also offers their cloud services through monthly and yearly plans for businesses. Their offering consists of three different packages that vary due to data requirements, number of websites and other analytic tools. Most users are based in Europe and the US.

While Innocraft is focused on becoming a sustainable business, it is doubtful whether privacy and security are selling points that can sustain the business in the long term. For this reason, the company is looking to develop other value propositions that align with their core values.

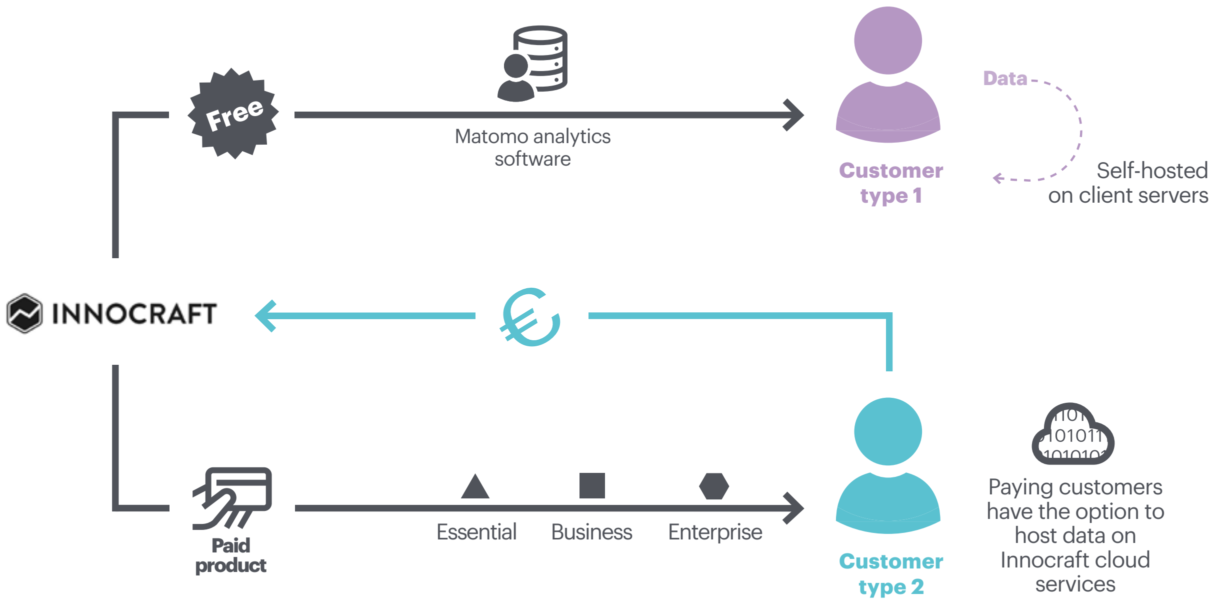

Free
Matomo analytics software
Customer type 1
Data
Self-hosted on client servers
INNOCRAFT
€
101 01011 101010
Paying customers have the option to host data on Innocraft cloud services
Paid product
Essential
Business
Enterprise
Customer type 2

Figure 8: The Innocraft business model.
Image source: Adapted from Business Model Toolbox
Data source: Innocraft 2019

Funding

Matomo began as a project under a different name, Piwik, and was funded by London-based company OpenX,[66] which at the time had a strong open-source strategy. OpenX was building an open-source ad server and bet on Aubry's web analytics project. After commissioning the project in 2007 and further developing Piwik later, they eventually sought external funding to sustain the project.

When Aubry left Piwik and created Matomo, he did so under Innocraft. The self-funded, New Zealand-based company quickly became profitable thanks to a small team and an open-source project that only monetised enterprise features. Aubry avoided seeking investment elsewhere as he had previously done with Piwik; he wanted to avoid the risk that investors would seek to control the open-source project.

Key takeaways

- Matomo is an alternative to Google Analytics. Marketing and analytics have evolved to embrace data-extractive models. Matomo provides businesses with solutions that help them analyse their website performance while complying fully with the GDPR.
- Matomo supports decentralisation as they give individuals and companies control over the data they track.
- A loyal user community is especially important to the success of open-source projects; Matomo relies on its community to resolve security issues, for example.
- The flexibility of a product allows users to adapt to different customer profiles regarding their technical know-how. Matomo can be used on-premise autonomously, but also provides expert technical support for those who need it.
- This flexibility also considers the size of different kinds of customers and their needs, from SMEs to large technology companies.

[66] OpenX 2019

3

Challenges and opportunities

Obstacles facing privacy-first business models

The companies presented in the case studies prove that it is possible to succeed with a business model that puts user privacy first. They share the common goal of raising awareness on exploitative business models rampant in the data economy, and their long-term strategy lies in building trust in their reimagined digital ecosystem by handling data transparently. The current data monetisation culture defines a playing field full of obstacles for alternative business models. These challenges are varied and interconnected.

Finding suitable funding

Financing is a primary concern for any new business. The most traditional route among digital start-ups is linked to venture capital. But these investors generally seek to support companies with the capacity to generate profits or scale quickly. However, as privacy-first business models are not based on the monetisation of data, exponential growth is not as feasible.

The four case examples show the variability and complexity of the path to find funding. DuckDuckGo was initially self-funded and then endorsed by venture capital investors. Nextcloud's founding team also self-funded the venture, while ProtonMail benefitted from the support of a privacy-conscious community to crowdfund the project along with venture capital injections and public funding. Initially incubated by a successful company, Matomo went through rounds of financing, and after "spinning out" was self-funded by its employees.

Given the culture of VC funding, value-driven businesses must look beyond traditional routes for investment. This includes exploring other sources of capital such as impact investing or crowdfunding. If they do opt for VC financing, privacy-first entrepreneurs must be aware of the terms and conditions under which the agreement is signed and the implications for their company. However, there is no single and prescriptive solution. ProtonMail and DuckDuckGo show that VC funding is also a possible route as long as values and objectives are aligned with investors.

Longevity

The case studies show how privacy-first businesses as value-driven ventures often experience tension between adhering to values and generating profits. For instance, Matomo and Nextcloud both faced internal struggles and conflicting business strategies. The pressure Matomo and Nextcloud face is two-fold: not only are they privacy-first, but they both have an open-source business model.

Open-source business models view communities of developers as both clients and key contributors, who collaboratively build, use and improve the software. In open-source, trust between management and the community is crucial to create a sustainable product. Jos Poortvliet, Nextcloud marketing director, stresses that earning money and going beyond volunteer work and donations is a big challenge for sustainable open-source business models.

Commitment to the community is something privacy-first companies are not willing to risk which can, at times, be burdensome. Data-extractive competitors see trust as secondary and can afford to since their product generates revenue despite the lack of trust. Since trust is core to their value proposition, privacy-first businesses must make tough decisions that may involve forgoing profit. ProtonMail CEO Andrew Yen explains:

> **"Most of this critical work [making a reliable and secure infrastructure] happens behind the scenes, but in terms of priority, it always comes ahead of new features. While everybody is understandably impatient for new features (we are too), if things take longer than expected, it is usually because we are investing in even more important infrastructure and anti-abuse capabilities."[67]**

Privacy-first companies expect slow growth, which also puts them in vulnerable positions and makes them easy targets for anti-competitive behaviour. According to ProtonMail, Google intentionally hid ProtonMail from search results for 10 months, causing its growth rate to decline 25% worldwide. From 2010 to 2018, Google also owned the URL duck.com which redirected users to Google search. They ceded duck.com to DuckDuckGo after the latter publicly complained on social media that Google was purposely confusing users.

High user acquisition cost

Companies with data-extractive business models are especially attractive to investors because the value of their product increases as their user base grows. Most successful platform businesses have network effects built into their business model. Instead, privacy-driven companies must seek alternative growth strategies that go beyond market niches and "free" culture.

Each of the four case study companies offer part (or all, in the case of DuckDuckGo) of their products or services for free and monetises extra features or technical support. A higher acquisition cost inhibits the otherwise strong network effect that free alternatives enjoy. In recent years, numerous projects offering privacy-based alternatives have failed for this reason, unable to reach a significant number of users that would enable them to compete with market leaders.[68]

To retain users, privacy-first companies must also offer a service at least as good as those offered by mainstream equivalents. As Nextcloud founder Frank Karlitschek explains, "You need to have all the features that the user expects."[69] He further explains that if the service does not have all the expected features, the user will go back to mainstream tools or search for another service.

[67] Yen 2018

[68] Newman 2018

[69] Mozilla 2019

Opportunities for privacy-first businesses

Although privacy-first companies face many challenges, there is a growing appetite for projects with an ethical approach to privacy and data.

Responding to social concerns about privacy

Data-driven companies have suffered numerous data breaches and security problems in recent years. These security flaws create a window of opportunity for business models with privacy at their core.

ProtonMail is an encrypted messaging alternative to Gmail, the world's most popular email service and the target of various attacks that have compromised the information of millions of users.[70] Nextcloud offers a self-hosted alternative to mainstream cloud storage options like Dropbox, victim of several cyberattacks that leaked passwords from their users. Matomo is an alternative to Google Analytics, a tool increasingly challenged by privacy-focused companies.[71]

The popularity of privacy-first businesses could grow in the coming years, especially since younger generations show greater awareness of privacy than their elders.[72] Governments are also showing a growing interest in privacy tools. Although some governments still use management tools built by large corporations,[73] more and more countries are demanding alternatives that guarantee data confidentiality and security.

A changing tech sector

A push for a more ethical tech is an emerging trend among the next generation of start-ups.[74] That is what the investment firm Union Square Ventures (USV) understood in 2011 when it met DuckDuckGo. "We invested in DuckDuckGo because we became convinced that it was not only possible to change the basis of competition in search, it was time to do it," explains Brad Burnham, partner at USV.[75]

This different approach to business is embodied by the movement Zebras Unite,[76] an organisation that promotes a more ethical and inclusive start-up culture. Zebras, as opposed to unicorns, are businesses that prioritise sustainable growth over exponential growth and the public interest over market domination.

Another growing trend in the tech sector is the rise of open-source as an increasingly popular method to develop and share technological solutions.[77] This movement, which is committed

[70] Johnson 2017

[71] Schwab 2019

[72] Raicu 2016

[73] Infobae 2016

[74] Montgomery 2019

[75] Burnham 2019

[76] Zebras Unite 2019

[77] Volpi 2019

to making technology available to everyone and embraces values such as transparency, is spreading among some governments and international organisations such as the United Nations through its United Nations Technology Innovation Labs (UNTIL).[78]

The need for specific solutions

Privacy-first companies may have a head start in sectors where data confidentiality and security are top priorities. The health and legal sectors deal with highly sensitive information and could benefit from solutions that protect user and industry data, especially since there are many business opportunities for these industries. Google's machine learning project for healthcare, code-named Nightingale, is one such example that shows the importance of privacy-first solutions. A November 2019 investigation revealed that not only were patients and doctors not informed of patient data use, but 150 Google employees were given access to sensitive health information.[79]

With privacy at the core of their business model, privacy-first businesses have the right mindset to be aware of these potential blunders. For example, ProtonMail recognises the sensitive nature of email exchange for certain professions and targets their marketing and communications to journalists, activists, government officials, and non-profit organisations, among others.[80]

Governments themselves show a growing interest in achieving maximum security in the control of their data and are taking measures to set up national data infrastructures. As illustrated in the previous section, Nextcloud responds to the French and German governments' needs to control their own data.[81] The French administration has also switched from Google to local and privacy-focused search engine Qwant.[82]

Current EU data protection legislation calls for concrete solutions to data centralisation. The European Data Protection Supervisor (EDPS) requires European institutions and governments to maintain control of the data and to know its whereabouts and purpose, even when processed by third parties. This requirement has called into question EU contracts with suppliers such as Microsoft, clearing a path for privacy-focused companies.[83]

[78] UNTIL 2019

[79] Fussell 2019

[80] Wolford 2019

[81] Nextcloud 2019

[82] Goujard 2018

[83] Lomas 2019

4

Taking action

Incentives for privacy-first business models

As we have seen, privacy-first companies face many challenges, the main one being their status as an exception in the tech industry. They face powerful rivals that benefit from network effects and proprietary tools. As a consequence, privacy-first businesses find it difficult to access funding and to become sustainable.

However, more and more market opportunities for companies that put privacy first are beginning to emerge. A growing number of businesses, governments and citizens are becoming aware of the importance of transparency and privacy when it comes to how technology companies use their data.

To leverage the opportunities presented in Section 3, policymakers must act. This report concludes with three initiatives that governments can implement to incentivise privacy-first businesses. These initiatives have been developed by the working group and respond to specific challenges these companies face.

Initiative 1: A privacy-first business certification

WHAT

An instrument to assess and certify privacy-first businesses would raise awareness about alternative business models and build consumer trust by "weeding out" privacy-washing initiatives. Creating a privacy-first certification using existing certifications (such as B-Corp[84]) as a template can incentivise governments, consumers and other businesses to support them.

WHY

As explained in the previous section, metrics designed to evaluate the potential success of a venture favour one type of company: one that prioritises exponential growth over sustainable growth. Value-driven business models are at a disadvantage as there is no holistic way to measure the success of a privacy-first business.

It is therefore urgent to create new metrics that measure business success beyond profit or number of users. The proposed certification would measure indicators such as sustainability, transparency, and protection of users' privacy rights, thereby reducing the complexity for governments who would like to contract privacy-first businesses.

The benefits of having a common certification are not only aimed at public servants. As consulting firm Edelman points out, "brands are now being pushed beyond their classic business interests to become advocates for a better society."[85] Several projects that evaluate the "privacy-friendliness" of tech companies already exist, such as "That one privacy site"[86] or PrivacySpy.[87] While these initiatives help raise consumer awareness about the importance of privacy in digital products and services, they have limited reach and have yet to see widespread adoption.

HOW

Creating a privacy-first certification requires a list of criteria that applicants must meet as well as an entity that accredits, monitors, and audits these companies.

A growing number of government initiatives mandated to oversee how data-driven technology affects society is another potential use case for such a certification. The Centre for Data Ethics and Innovation in the UK and Denmark's Council for Data Ethics are two government-led initiatives that gather experts from various sectors to advise policymakers on technological governance. These government-led entities could serve as models for a secretariat that promotes and administers a privacy-first certification.

This supervisory role could later be carried out by an organisation at the regional or global level that guarantees compliance with the agreed certification criteria. This entity would certify independent accreditation agencies that would be responsible for assessing whether a company meets the agreed criteria. The role of the secretariat would be to monitor these independent certification agencies and ensure they comply with standards. In order to ensure accountability and transparency, the secretariat should be supervised by:

- A board of experts that agrees on the criteria that underlie the certification
- Two advisory committees: one composed of citizens and another of government representatives
- An auditor, which evaluates independently if the accreditation agencies are meeting the standards set by the secretariat

To create this governance structure, it is important to avoid possible conflicts of interest between elected secretariat members. Also, policymakers must be mindful to choose a diverse group of stakeholders that represent the digital business sector.

Once the self-regulated structure is in place, the board of experts should determine a set of certification standards designed to evaluate whether the business model is based on the monetisation of data and whether its activity contributes to a competitive market. Additionally, the board should establish and communicate a clear certification process and determine the frequency of audits.

[84] Bcorporation.net 2019

[85] Edelman 2019

[86] Thatoneprivacysite.net 2019

[87] PrivacySpy 2019

Initiative 2: Procuring privacy-first businesses

WHAT

The public sector can directly influence digital markets by setting an example. One way is to use public procurement to contract companies that handle user data responsibly.

Including a specific requirement in public procurement processes requires establishing criteria and testing them incrementally by sector. For instance, the initiative could be piloted within two specific areas of public services: health and education. Transparency and privacy are especially relevant to these sectors whose beneficiaries include vulnerable groups that governments are mandated to protect. The initiative could eventually be extended to other areas of public administration, according to the results obtained in the pilot testing of the health and education sectors.

WHY

Public spending holds significant purchasing power; it accounts for 12% of GDP in OECD countries and up to 30% in developing countries.[88] Shifting public spending towards more responsible technology companies could increase the visibility of privacy-first businesses and drive new markets — led by the public sector — to companies that do not base their business on data monetisation.

Public procurement as a lever to incentivise business model innovation is not without precedent. For years, the European Commission has mandated the public procurement of "goods, services and works with a reduced environmental impact throughout their life cycle."[89] In addition to its direct impact on the environment, Green Public Procurement (GPP) has brought numerous benefits to the regions where it has been implemented, such as higher environmental performance standards, as well as economic benefits including industry innovation, increased competition, and reduced prices.[90]

[88] UN Environment Programme n.d.

[89] Ec.europa.eu 2019

[90] Ibid.

HOW

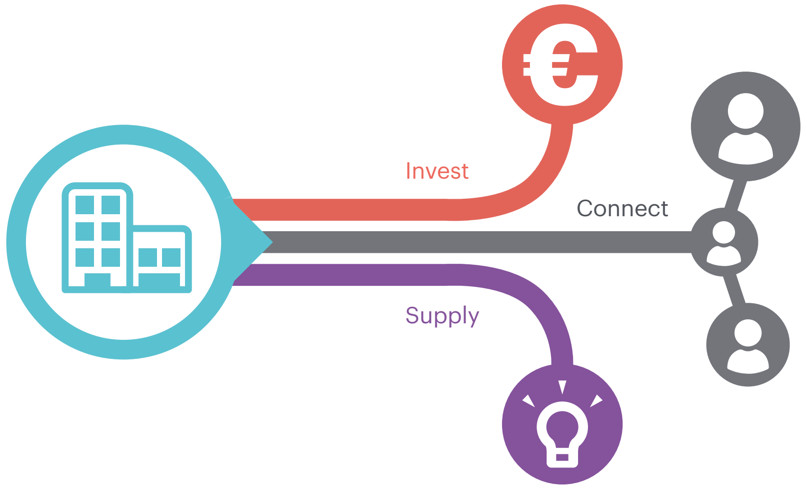
Policymakers can create a public procurement requirement that encourages public administration to contract privacy-first businesses using a soft regulatory approach. This would mean contracting a privacy-first company would not be a requirement but rather a default option; procurement officers would have to justify their decision to opt out.

To further promote the use of privacy-first businesses, independent auditors or third-party researchers could monitor which government agencies or departments contract privacy-first businesses.

Initiative 3: A global network of privacy-first incubators

WHAT

Business incubators can be instrumental in stimulating an emerging sector or type of company, such as financial technology (FinTech). While many are privately funded, other incubators and entrepreneur networks are funded with public resources. One example is EIT Climate-KIC, a programme supported by the European Commission that works to accelerate the transition to a zero-carbon economy.[91] Through a specific programme for entrepreneurs with climate-related business ideas, Climate-KIC offers business development support and organises international competitions that reward the best ideas. Since its 2009 launch, Climate-KIC has supported 2,000 start-ups, creating one of the largest entrepreneurial communities in the world.[92]



[91] Climate-kic.org 2019

[92] Ibid.

Following the Climate-KIC model, a global network of privacy-first business incubators would:

- Support and finance privacy-first business ideas exclusively. Participating ventures must be open, replicable, and scalable projects with solutions to deliver privacy, security, and transparency to their users.
- Build an international ecosystem of digital companies with a focus on privacy, trust, and transparency in the use of data.
- Create a physical (third) space for collaboration aligned with the privacy-first ethos.

WHY

Among the most complex challenges that privacy-first businesses face is funding. Creating an incubator that specifically supports this type of business can facilitate contact with value-minded impact investors, which are also on the rise.[93]

An incubator dedicated to digital companies focused on privacy would also serve to monitor the evolution of these businesses and ensure they remain true to their initial values.[94]

In addition to supporting the entrepreneurs involved, a privacy-first incubator could normalise the responsible use of data among young entrepreneurs in the technology sector. An incubator squarely focused on this type of company could support the evolution of the technology sector towards a new set of values that include privacy, transparency and trust as primary goals.

Additionally, the incubator could serve as a hub for a global network of similar projects that feed this ecosystem, helping to establish a new international paradigm for digital business.

Not only would such an ecosystem serve as a neutral space for diverse stakeholders (the public and private sectors, research institutions and civil society organisations) to collaborate, but can also facilitate the construction of diverse teams. For instance, an incubator network can serve as a channel to connect privacy-first technology with the needs of governments in areas such as health, education, environment, etc. These collaborations can be designed to achieve useful privacy-first solutions that can be implemented at scale and can be customised for different realities and cultural contexts.

[93] Preston and James 2019

[94] Nesta 2014

HOW

The roadmap to creating a global network of privacy-first business incubators entails a stepwise approach.

1 Identify the key stakeholders from academia, regional organisations from civil society and the private sector, specifically privacy-first companies such as those analysed in Section 2, to become partners of the initiative.

2 Form an advisory board to draft and validate a privacy-first declaration or terms of reference document, which would set requirements participant companies would need to meet in order to participate.

3 Obtain endorsements and financial support from governments with existing institutional resources and channel them to the incubator network. Governments can kickstart the global network by choosing municipal governments that already have strong entrepreneurial ecosystems. The global network can collaborate with existing ones, such as the Small Business Development Centers in the United States or the European Business and Innovation Centres Network. Instead of starting from scratch, these public-led networks can become a referral point for business plan development and administrative support, accounting and legal services, from which privacy-first businesses can benefit.

4 Launch the declaration, network and fund with key incubators through an open call for privacy-first business solutions.

5 Scale worldwide through events (hackathons, career fairs, conferences or awards) to attract new partners to the network.

Incubating privacy-first companies using public resources would ensure that public funds go to initiatives with social impact, such as in this case, the protection of citizens' data. A potential challenge would be ensuring privacy-conscious business models do not morph into data extractive models after completing the incubator programme.

Conclusion

Towards a privacy-first digital future

Through an in-depth exploration of privacy-first businesses, this report has shed light on an emerging type of company, one that can profitably offer digital products and services without employing invasive data-handling practices. The challenges privacy-first businesses face are shared by any small player entering a monopolised market. However, stronger recognition together with the financial resources to defend their value-driven mission can catalyse the success of these companies while providing a competitive case for a more private internet.

Nonetheless, competition is fierce. Privacy-first businesses can only ride the techlash wave so far, as big tech companies enjoy seemingly limitless resources to influence regulations and define the direction of the technology sector. Still, this report has shown how privacy-first companies are not playing a zero-sum game. Like other value-driven ventures, they seek to prove that privacy and profit are not mutually exclusive. This is not an easy task given how the existing culture favours companies that project exponential growth.

Recognising the potential of privacy-first businesses, the initiatives designed by the working group seek to address the specific needs of these companies, such as greater visibility and more resources. The certification, procurement guidelines and incubator initiatives are all based on existing instruments that policymakers have used to incentivise other sectors, such as the green economy. While these initiatives are not entirely new, they have been adapted so that policymakers can implement them based on their specific context.

Given the rapid pace of technological change, the next few years will be critical for the survival of the nascent privacy-first ecosystem. In order to effectively nurture this ecosystem, policymakers must be able to identify and understand the complexity of these new business models and build upon incentives. Most importantly, they must recognise the inherent value and expertise already within profitable privacy-first businesses like the ones covered in this report in order to guide other privacy-first ventures to thrive.

References

Asher Hamilton, I. (2018). Tim Cook mounted his most stinging attack yet on tech firms that hoard 'industrial' quantities of data. Business Insider. [online] Available at: https://www.businessinsider.es/apple-ceo-tim-cook-attacks-tech-firms-that-hoard-data-2018-10?r=US&IR=T

Bcorporation.net. (2019). Certified B Corporation. [online] Available at: https://bcorporation.net/

Bhartiya, S. (2016.) Dark cloud looms over ownCloud as founder resigns. CIO. [online] Available at: https://www.cio.com/article/3063519/dark-cloud-looms-over-owncloud-as-founder-resigns.html

Brandel, J., Zepeda, M., Scholz, A. and Williams, A. (2017). Zebras: Let’s Get In Formation. Medium. [online] Available at: https://medium.com/@sexandstartups/zebras-lets-get-in-formation-fdcbc72fec4a

Burnham, B. (2011). Duck Duck Go. Union Square Ventures. [online] Available at: https://www.usv.com/writing/2011/10/duck-duck-go

Chan, N. (2019). 259: Taking on Google, with Gabriel Weinberg, Founder of Privacy Browser DuckDuckGo. Foundr. [online] Available at: https://foundr.com/gabriel-weinberg-duckduckgo

Climate-kic.org. (2019). Entrepreneurship - Climate-KIC. [online] Available at: https://www.climate-kic.org/programmes/entrepreneurship

Climate-kic.org. (2019). KIC: The EU's main climate innovation initiative. Climate-KIC. The EU's main climate innovation innovation initiative. [online] Available at: https://www.climate-kic.org

Couldry, N. (2016). The price of connection: 'surveillance capitalism'. The Conversation. [online] Available at: https://theconversation.com/the-price-of-connection-surveillance-capitalism-64124

Digitalcooperation.org. (2019). The age of digital interdependence. [PDF] Available at: https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-web-FINAL-1.pdf

Downes, L. (2019). GDPR and the End of the Internet’s Grand Bargain. Harvard Business Review. [online] Available at: https://hbr.org/2018/04/gdpr-and-the-end-of-the-internetsgrand-bargain

DuckDuckGo. (2019). Open Source Overview. [online] Available at: https://help.duckduckgo.com/duckduckgo-help-pages/open-source/opensource-overview

DuckDuckGo. (2019). DuckDuckGo Privacy. [online] Available at: https://duckduckgo.com/privacy

DuckDuckGo. (2019). Privacy, simplified. - DuckDuckGo Browser Extension & Mobile App. [online] Available at: https://duckduckgo.com/app

Ec.europa.eu. (2019). Benefits of GPP. Benefits - GPP - Environment - European Commission. [online] Available at: https://ec.europa.eu/environment/gpp/benefits_en.htm

Edelman. (2019). Earned Brand 2018. Edelman. [online] Available at: https://www.edelman.com/earned-brand

Etherington, D. (2019). Apple is now the privacy-as-a-service company. TechCrunch. [online] Available at: https://techcrunch.com/2019/06/03/apple-is-now-the-privacy-as-a-service-company

European Union Agency for Network and Information Security. (2018). Recommendations on shaping technology according to GDPR provisions. [online]. Available at: https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions

Faravelon, A., Frenot, S. and Grumbach, S. (2015). Chasing Data in the Intermediation Era: Economy and Security at Stake. IEEE Security & Privacy. [PDF] Available at: https://www.researchgate.net/publication/281599782_Chasing_Data_in_the_Intermediation_Era_Economy_and_Security_at_Stake

Fussell, S. (2019). Google's Totally Creepy, Totally Legal Health-Data Harvesting. The Atlantic. [online] Available at: https://www.theatlantic.com/technology/archive/2019/11/google-project-nightingale-all-your-health-data/601999

GDPR.eu. (2019). What are the GDPR consent requirements? - GDPR.eu. [online] Available at: https://gdpr.eu/gdpr-consent-requirements/

General Data Protection Regulation (GDPR). (2019). Art. 83 GDPR – General conditions for imposing administrative fines | General Data Protection Regulation (GDPR). [online] Available at: https://gdpr-info.eu/art-83-gdpr/

Github. (2019). DuckDuckGo. GitHub. [online] Available at: https://github.com/duckduckgo

Goujard, C. (2018). France is ditching Google to reclaim its online independence. WIRED. [online] Available at: https://www.wired.co.uk/article/google-france-silicon-valley

GSMA. (2018). The Data Value Chain. [PDF] Available at: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/06/GSMA_Data_Value_Chain_June_2018.pdf

GSMA. (2018).The Mobile Economy 2018. [PDF] Available at: https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf

Herrle, J. and Hirsh, J. (2019). The Peril and Potential of the GDPR. Centre for International Governance Innovation. [online] Available at: https://www.cigionline.org/articles/peril-and-potential-gdpr

Infobae. (2016). El Gobierno utilizará la versión corporativa de Facebook para agilizar el trabajo interno. [online] Available at: https://www.infobae.com/2016/02/16/1790481-el-gobierno-utilizara-la-version-corporativa-facebook-agilizar-el-trabajo-interno

International Data Corporation. (2019). IDC Forecasts Revenues for Big Data and Business Analytics Solutions Will Reach $189.1 Billion This Year with Double-Digit Annual Growth Through 2022. [online] Available at: https://www.idc.com/getdoc.jsp?containerId=prUS44998419

Johnson, A. (2017). Massive phishing attack targets millions of Gmail users. CNBC. [online] Available at: https://www.cnbc.com/2017/05/04/gmail-google-hack-phishing-attack.html

Jones, H. (2018). Dr. Ann Cavoukian: Why Big Business Should Proactively Build for Privacy. Forbes. [online] Available at: https://www.forbes.com/sites/cognitiveworld/2018/08/17/ann-cavoukian-why-big-business-should-proactively-build-for-privacy/#92dcc5c2e3d8>

Karlitschek, F. (2016). Big changes: I am leaving ownCloud, Inc. today. Frank Karlitschek RSS. [online] Available at: https://karlitschek.de/2016/04/big-changes-i-am-leaving-owncloud-inc-today

Lomas, N. (2018). DuckDuckGo gets $10M from Omers for global privacy push. TechCrunch. [online] Available at: https://techcrunch.com/2018/08/29/duckduckgo-gets-10m-from-omers-for-global-privacy-push

Lomas, N. (2018). Pro-privacy search engine DuckDuckGo hits 30M daily searches, up 50% in a year. TechCrunch. [online] Available at: https://techcrunch.com/2018/10/11/pro-privacy-search-engine-duckduckgo-hits-30m-daily-searches-up-50-in-a-year/

Lomas, N. (2019). EU contracts with Microsoft raising 'serious' data concerns, says watchdog. TechCrunch. [online] Available at: https://techcrunch.com/2019/10/21/eu-contracts-with-microsoft-raising-serious-data-concerns-says-watchdog

Ly, W., Nirei, M., and Yamana, K. (2019). Value of Data: There's No Such Thing as a Free Lunch in the Digital Economy. The Research Institute of Economy, Trade and Industry. [PDF] Available at: https://www.rieti.go.jp/en/publications/summary/19030027.html

Matomo. (2019). Matomo Security Bug Bounty Programme. Matomo. [online] Available at: https://matomo.org/security

Matomo. (2019). New to Piwik FAQ - Analytics Platform. Matomo. [online] Available at: https://matomo.org/faq/new-to-piwik/#faq_130

Mazzucato, M. (2015). From Market Fixing to Market-Creating: A New Framework for Economic Policy. SPRU Working Paper Series (SWPS), 2015-25: 1-19. [PDF] Available at: https://www.sussex.ac.uk/webteam/gateway/file.php?name=2015-25-swps-mazzucato.pdf&site=25

Mazzucato, M. (2017). The entrepreneurial state. [PDF] Available at: https://marianamazzucato.com/wp-content/uploads/2017/02/US-ES-intro.pdf

Montgomery, M. (2019). Techlash Backlash? Next Generation of Startups Infusing Ethics Into Its Roots. Forbes [online] Available at: https://www.forbes.com/sites/mikemontgomery/2019/11/19/techlash-backlash-next-generation-of-startups-infusing-ethics-into-its-roots/#11cb18a04c16

Mozilla. (2019). An open source alternative for "the cloud". [online] The Internet Health Report 2019. Available at: https://internethealthreport.org/2019/an-open-source-alternative-for-the-cloud

Naughton, J. (2019). 'The goal is to automate us': welcome to the age of surveillance capitalism. The Guardian. [online] Available at: https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

Nesta. (2014). Startup Accelerator Programmes. A Practice Guide. [PDF] Available at: https://media.nesta.org.uk/documents/startup_accelerator_programmes_practice_guide.pdf

Newman, J. (2018). The Dream of a Privacy-First Social Network: 6 Alternatives to Facebook. Fast Company. [online] Available at: https://www.fastcompany.com/40559106/the-privacy-first-social-network-a-great-idea-that-never-works

Nextcloud. (2019). EU governments choose independence from US cloud providers with Nextcloud. [online] Available at: https://nextcloud.com/blog/eu-governments-choose-independence-from-us-cloud-providers-with-nextcloud/

Nextcloud. (2019). How Nextcloud keeps your data secure. Nextcloud. [online] Available at: https://nextcloud.com/secure

Nytimes.com. (2019). Opinion | The New Terminology for Privacy. [online] Available at: https://www.nytimes.com/interactive/2019/04/10/opinion/internet-privacy-terms.html

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. UCLA l. Rev., 57, 1701.

Opensource.org. (2019). The Open Source Definition | Open Source Initiative. [online] Available at: https://opensource.org/osd

OpenX. (2019). About OpenX: Global Leader in Programmatic Advertising. OpenX. [online] Available at: https://www.openx.com/company/

Piwik. (2019). Piwik is now Matomo! [online] Available at: https://piwik.com/

Poortvliet, J. (2016). Building a business on a solid open source model. Opensource.com. [online] Available at: https://opensource.com/business/16/6/building-business-solid-open-source-model

Poortvilet, J. (2019). Nextcloud Conference 2019 talks now online. [online] Nextcloud. Available at: https://nextcloud.com/blog/nextcloud-conference-2019-talks-now-online

Preston, M. and James, M. (2019). What Does the Growth of Impact Investing Mean? Harvard Law School Forum on Corporate Governance and Financial Regulation. [online] Available at: https://corpgov.law.harvard.edu/2019/11/10/what-does-the-growth-of-impact-investing-mean/

PrivacySpy. (2019). About | PrivacySpy. [online] Available at: https://privacyspy.org/about/

ProtonMail. (2015). Is ProtonMail trustworthy? Our thoughts on email trust. ProtonMail Blog. [online] Available at: https://protonmail.com/blog/is-protonmail-trustworthy/

ProtonMail. (2015). ProtonMail Open Source Cryptography. ProtonMail Blog. [online] Available at: https://protonmail.com/blog/protonmail-open-source-crytography/

ProtonMail. (2019). Pricing. ProtonMail. [online] Available at: https://protonmail.com/pricing

ProtonMail. (2019). ProtonMail is expanding access to more Android users. ProtonMail Blog. [online] Available at: https://protonmail.com/blog/android-expansion/

Raicu, I. (2016). Young adults take more security measures for their online privacy than their elders. Vox. [online] Available at: https://www.vox.com/2016/11/2/13390458/young-millennials-oversharing-security-digital-online-privacy

Sadowski, J. (2019). When data is capital: Datafication, accumulation, and extraction. Big Data & Society, 6(1).

Sawers, P. (2018). How ProtonMail is pushing email privacy standards. VentureBeat. [online] Available at: https://venturebeat.com/2018/05/13/how-protonmail-is-pushing-email-privacy-standards

Schwab, K. (2019). It's time to ditch Google Analytics. Fast Company. [online] Available at: https://www.fastcompany.com/90300072/itstime-to-ditch-google-analytics

Shacklett, M. (2018). 5 ways to avoid vendor lock-in. TechRepublic. [online] Available at: https://www.techrepublic.com/article/5-ways-to-avoid-vendor-lock-in/

Sec.gov. (2006). [online] Available at: https://www.sec.gov/Archives/edgar/data/1142701/000110465906033409/a06-9620_110q.htm

Slade, H. (2014). The Only Email System The NSA Can't Access. Forbes. [online] Available at: https://www.forbes.com/sites/hollieslade/2014/05/19/the-only-email-system-the-nsa-cant-access/#728c6c0867f7

StatCounter. (2019). Search Engine Market Share Worldwide. StatCounter Global Stats. [online] Available at: https://gs.statcounter.com/searchengine-market-share#yearly-2019-2019-bar

Sugiyama, S. (2019). Abe heralds launch of 'Osaka Track' framework for free cross-border data flow at G20. The Japan Times. [online] Available at: https://www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20/#.XfoXimRKiUl

Thatoneprivacysite.net, (2019). VPN Comparison. That One Privacy Site. [online] Available at: https://thatoneprivacysite.net

UN Environment Programme. (n.d.). Sustainable consumption and production policies. [online] Available at: https://www.unenvironment.org/explore-topics/resource-efficiency/what-we-do/sustainable-consumption-and-production-policies

Un.org. (2019). Data Economy: Radical transformation or dystopia? [PDF] Available at: https://www.un.org/development/desa/dpad/wp-content/uploads/sites/45/publication/FTQ_1_Jan_2019.pdf

Unctad.org. 2019. Data Protection and Privacy Legislation Worldwide. UNCTAD. [online] Available at: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Until.un.org. (2019). Home Technology Innovation Labs. United Nations. [online] Available at: https://until.un.org

Volpi, M. (2019). How open-source software took over the world. [online] TechCrunch. Available at: https://techcrunch.com/2019/01/12/how-open-source-software-took-over-the-world

Wachter, S. (2019). Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. SSRN Electronic Journal.

Weinberg, G. (2011). Are you chasing a fad or a market? Gabriel Weinberg’s blog. [online] Available at: https://web.archive.org/web/20181204131004/https://ye.gg/blog/2011/04/are-you-chasing-a-fad-or-a-market.htm

Wilson, M. and Graham, M. (2013). Neogeography and Volunteered Geographic Information: A Conversation with Michael Goodchild and Andrew Turner. Environment and Planning A: Economy and Space, 45(1), pp.10-18.

Wolford, B. (2019). Using ProtonMail for Journalism. ProtonMail Blog. [online] Available at: https://protonmail.com/blog/journalism

Yen, A. (2015). ProtonMail has raised $2M USD to protect online privacy. ProtonMail Blog. [online] Available at: https://protonmail.com/blog/protonmail-has-raised-2m-usd-to-protect-online-privacy

Yen, A. (2018). A look back at 2018 and our vision for the future of ProtonMail. ProtonMail Blog. [online] Available at: https://protonmail.com/blog/2018-recap-future-roadmap

Yen, A. (2019). We have been awarded €2 million from the EU to further develop the Proton ecosystem. ProtonMail Blog. [online] Available at: https://protonmail.com/blog/eu-funding

Zebras Unite. (2019). Zebras Unite. [online] Available at: https://www.zebrasunite.com

Zuboff, S. (2019). The age of surveillance capitalism. London: Profile Books, pp.75-77.

Acknowledgements

Coordinating author

- **Tanya Alvarez** - Researcher, Digital Future Society Think Tank

Expert contributors

This report draws on the expertise and inputs of the following expert contributors:

- **Ali Hussein** – Kenya ICT Action Network (KICTANet)
- **Ayden Ferderline** – Mozilla Fellow
- **Carles Barreiro Bertolí** – Lawyer and DPO, Barcelona Bar Association (ICAB)
- **Cristian Barrué** – Post-doctoral researcher, Universitat Politècnica de Catalunya
- **Molly Wilson** – Senior Researcher & Designer, Simply Secure
- **Pieter van Boheemen** – Researcher, Rathenau Instituut
- **Renata Ávila** – Director, Ciudadanía Inteligente
- **Tetsuro Narita** – Inter-American Development Bank
- **Frank Karlitschek** – Founder, Nextcloud
- **Johnny Ryan** – Chief Policy & Industry Relations Officer, Brave
- **Mattieu Aubry** – Founder, Innocraft
- **R. Miles McCain** – Founder, PrivacySpy
- **Rory Donnelly** – CEO, Digi.Me

Digital Future Society Think Tank team

Thank you to the following Digital Future Society Think Tank colleagues for their input and support in the production of this report:

- **Carina Lopes** – Head of the Digital Future Society Think Tank
- **Nicole Harper** – Editor, Digital Future Society Think Tank
- **Olivia Blanchard** – Researcher, Digital Future Society Think Tank

Citation

Please cite this report as:

- Digital Future Society. (2019). Privacy-first: a new business model for the digital era. Barcelona, Spain.

Appendices

Appendix I: How to spot privacy-first businesses

The following characteristics can be used to identify privacy-first businesses. They are:

1 For the user: the user is the main beneficiary of this model

- Users have complete control over their data, except for when the business is required by law to disclose data.
- The business is designed to collect minimal to no data. It can prove that it collects no more than the minimal data required to carry out the service it provides.
- The user can either store data on their device or on a cloud/service to which the company has no direct access. The company discloses the security measures taken if data is stored outside of the users' device/server and only stores data for a limited time.
- The business allows users to choose whether the software or service uses their data in the first place.

2 Clear communicators

- Users are informed of every step of the data collection process. Explicit, plain language is used to explain what type of data is collected, how it is collected and for what purpose, how it is handled and how the user can exercise control over the data (if applicable).

3 Private by Design

- The product or service protects user privacy by default.

4 Aligned with data processors

- As privacy-first companies handle personal data as little as possible, there is little to no data handling outside of the business. If third parties are involved, the data they deal with is not traceable, as the data initially collected is not identifiable by the company itself. Any affiliate third party that may require access to user data is vetted by the business.

5 Secure

- Data security is part of the value proposition. Security protocols are transparent and available for review.

6 Accountable

- The business has technical and organisational measures in place to prove that it is privacy-first. Additionally, businesses are proactive in their communication to the community and stakeholders.

Appendix II: What is personal data?

This report explores the ways in which business models can generate revenue without the use of personal data. The table below describes how data is categorised under the current GDPR regulation.

<table>
<tr><td colspan="2"><b>Personal data</b>
Any public or private information that can be traced back or used to identify a person, directly or indirectly.
Examples: cultural, physiological, social attributes</td><td rowspan="3"><b>Non-personal data</b>
Constitutes most of the data generated, usually created by a machine or systems.

Examples: performance data, transactions, individual data that is anonymised.</td></tr>
<tr><td><b>Volunteered</b>
Data the subject is aware of giving up.

Examples: sensitive information that you may give your bank or medical provider, such as ID or social security number. Social media content. It also includes location data if applications are set to geolocate posts.[95]</td><td rowspan="2"><b>Inferred</b>
New insights taken from volunteered and observed data.

Data that feeds into algorithms that recommend a product to a user, calculate credit ratings, profiles, etc.</td></tr>
<tr><td><b>Observed</b>
Metadata or user data collected through the services a person uses.

Examples: Mobile phone billing data, metrics on website use, location.</td></tr>
</table>

[95] Wilson & Graham 2013

Appendix III: Mapping the global privacy-first ecosystem

Privacy-first for-profits

Business name	Location	Type	Description
Brave	US	B2C/B2B	An open-source browser that blocks ads/"unwanted content" and secures privacy. Claims to be 8x faster than Chrome and Safari.
Cozycloud	France	B2C	A private server to store personal data and personal web apps. Besides privacy and security, they claim to offer easy-to-use and intelligent data storage.
Clue	Germany	B2C	Period and ovulation tracking app. Clue anonymises data and sends it to research institutions to advance the study of women's health and fertility.
Fathom	US-based	B2C/B2B	Privacy conscious analytics platform. Provides useful website statistics without tracking or storing users personal data. It anonymises visitors using hashes, does not use cookies and is GDPR/PECR compliant.
MaidSafe	Scotland	B2C/B2B	Project SAFE (Secure Access for Everyone) seeks to replace the centralised and controlled internet with a fully decentralised and trustless network. It is an open-source project that provides users with a fully decentralised solution.
OpenCollective	US	B2C	Platform that enables groups and communities to collect and disburse money transparently. Promotes financial transparency. Helps organisations collect money without needing a bank account or creating a legal entity.
Purism	US	B2C/B2B	Security-focused computing devices. Purism offers bundles of services including email, social media, a VPN and end-to-end encryption. They also build laptops and phones that protect privacy. All software is open-source and easily auditable, all source code is public, no backdoors or need to register. It is modifiable according to user needs.

Business name	Location	Type	Description
Threema	Switzerland	B2B/B2C	End-to-end encrypted instant messaging application that does not ask for any personally identifiable information. Several privacy-related features (full anonymity, comprehensive encryption, transparent privacy policy, etc.) are part of the value proposition.
Tresorit	Hungary/ Switzerland	B2B/B2C	Cloud storage service that emphasises enhanced security and data encryption. Helping companies to store and share their files and data, following compliance and privacy principles.
Wickr	US	B2B/B2G	Software company mostly known for its highly-secure instant messenger application. They also offer a full communication platform, end-to-end encrypted, under the Wickr Pro brand.
Qwant	France	B2C	Search engine with its own indexing engine (only EU-based) that claims not to track users and avoids the creation of filter bubbles by not personalising searches. User-friendly search engine, free to use and privacy-first. Offers "Qwant junior" for children (filters results).

Privacy-first non-for-profits

Name	Country	Description
Freenet	N/A	Peer-to-peer platform to avoid censorship, using a decentralised distributed data store to keep and deliver information. Communication is encrypted and routed through other nodes to make it extremely difficult to determine who is requesting the information and what its content is.
Midata	Switzerland	Cooperative that gives people control over their medical data. They can safely store it, track their progress and, if they want, share it with their doctor, family or clinical trials. Platform that empowers users to use their data to advance health research.
OpenStreetMap	UK (OpenStreetMap Foundation)	A collaborative project to create a free and editable map of the whole world. The maps are based on crowdsourced data collected by users.
Securedrop	N/A	Platform for secure communications between media/journalists and whistleblowers (exposed sources). Useful tool for media organisations to accept documents from anonymous sources.
Signal	US	An encrypted messaging service that can be used for one-to-one and group communications. Users can verify the identity of their contacts and the integrity of the data channel. Runs on any mobile platform.
Solid	US	Led by Sir Tim Berners Lee. A platform that allows users to read and create content while managing data accessibility. Gives users control over data and users can decide what apps have access to it.
Telegram	UK/UAE	A cloud-based messaging and voice over IP service. Messages, photos, videos, audios and any other kind of file can be sent through the app. Users can access messages and files from several devices and share heavy photos.

Digital
Future Society