The Impact of Privacy Laws on Everyday Life in Switzerland: A Social Perspective

Kenan Henzelin

Haaga-Helia University of Applied Sciences
Business Information Technology
Bachelor's Thesis
2024

Abstract

Author(s)
Kenan Henzelin

Degree
Bachelor of Business Information Technology

Report/Thesis Title
The Impact of Privacy Laws on Everyday Life in Switzerland: A Social Perspective

Number of pages and appendix pages
73 + 6

This thesis explores the impact of privacy laws on everyday digital life in Switzerland from a social perspective, with a particular focus on the relationship between digital rights, public awareness, and personal empowerment. In a society where digital interactions are omnipresent and data collection is increasingly pervasive, understanding the societal role and reception of privacy regulations such as the Swiss Federal Act on Data Protection (FADP) and the European GDPR is more important than ever.

The aim of this research is to assess how individuals perceive, understand, and interact with privacy laws, and to identify whether these laws effectively support digital sovereignty at both governmental and personal levels. The study also investigates the extent to which the general population feels equipped to exercise control over their digital presence and data.

The theoretical framework introduces the core concepts of privacy, data protection, digital literacy, trust in digital systems, and digital sovereignty. These notions are contextualized within current literature and examined through a socio-technical lens, with references to scholars such as Zuboff and Fratini, who highlight the growing tension between individual autonomy and corporate or governmental data control.

In the empirical part, the author combines a quantitative survey targeting the general population with a qualitative interview conducted with a cybersecurity expert in the financial sector. The survey investigates levels of awareness, behavior, and attitudes related to privacy rights and digital sovereignty, while the expert interview provides insights into the practical challenges and ethical considerations of implementing data protection in a heavily regulated industry.

The results indicate a significant gap between legal provisions and public understanding. While privacy is widely valued in theory, there is limited practical engagement with legal rights and digital tools. Trust in institutions and major tech platforms is fragile, and many respondents express the need for clearer information and more accessible means to protect their data.

Based on these findings, the thesis proposes several improvements: integrating digital rights into education, simplifying access to data rights, promoting privacy-friendly alternatives, and fostering collaboration between public institutions, academia, and civil society. These suggestions are aimed at reducing the disconnect between regulation and lived experience, and at strengthening both individual and collective digital sovereignty.

The reliability and validity of the research are considered through its methodological design and mixed-methods approach. The study contributes to the broader discourse on digital citizenship by highlighting the importance of social understanding and engagement in the successful implementation of privacy legislation.

Key words
data protection, privacy, social empowerment, digital sovereignty, legislation, Switzerland

Table of Contents

1 Introduction

1.1 Background

Even before what we could call the digital age, privacy as always been a foundational democratic principle, putting forward the freedom and trust that should be the most basic right in any society. Nowadays, the technologic advancements gave those concepts even more importance. This raises questions about the collection, storage, and use of personal data. For that reason, governments and organizations are slowly trying to push forward legal and societal changes to further protect people while seeking a balance between technological innovation and the protection of individual rights.

However, privacy laws are among the most intricate fields of modern legislation. The constant evolution of technology forces a rapid pace of changes. While trying to protect individuals from the misuse of their personal data, lawmakers must understand and assess the threat of new technologies on an almost daily basis. Unfortunately, their complexity often makes them difficult for the general population to fully understand, leaving a significant gap between legislative intent and societal understanding.

Switzerland is a unique country in Europe. Its position at the crossroads of national sovereignty and international cooperation makes it an interesting case study for exploring the impact of data protection laws. The FADP, the Swiss Federal Act on Data Protection, which was recently revised in 2023 to work in tandem with the GDPR, European Union's General Data Protection Regulation, aims to protect personal and sensitive data while ensuring transparency and accountability. These laws are aimed at companies and public institutions but have a major impact on the lives of citizens by shaping their interactions with technology and their perceptions of privacy.

The general public's lack of awareness or understanding of these laws poses a significant challenge. For many, privacy laws are abstract, perceived as dense legal texts that feel disconnected from their everyday realities. This lack of knowledge limits individuals' ability to exercise their rights, protect their data, and engage critically with digital services. Furthermore, misconceptions or lack of understanding can lead to mistrust in institutions and uncertainty about the effectiveness of such regulations.

This disconnection between the complexity of privacy laws and the population's understanding of them underscores the need for a social study that investigates their tangible impact on daily life.

Despite their significance, the social impact of privacy laws remains underexplored. While legal and technical analyses have been proliferating for the last few years, there is a lack of research examining how these regulations affect the behaviors, attitudes, and daily experiences of ordinary individuals.

1.2 Research Question, Objective & Investigative Questions

As explained previously, the lack of awareness among the general population makes it difficult for lawmakers and experts in the field to enforce data protection. This means that an individual understanding of their rights is necessary for people to be truly protected. The overall goal of this thesis is to investigate the social impact and awareness of privacy laws. This study will focus mostly on the FADP, the Swiss Federal Data Protection Act, which works in tandem with the GDPR, the European Union's General Data Protection Regulation. By examining the practical implications of these laws, the thesis aims to bridge the gap between legislative intent and societal understanding.

RQ: What is the societal impact of privacy laws like the FADP and GDPR on individuals in Switzerland?

RO: The research aims to analyze the impact of privacy laws on the daily lives of Swiss citizens, focusing on their understanding, attitudes, and behaviors toward digital privacy, while exploring ways to bridge the knowledge gap.

IQ1: How does the public perceive and interact with privacy laws in Switzerland?

IQ2: What societal impacts do privacy laws have on citizens' daily lives and their trust in institutions?

IQ3: How can the complexity of privacy laws be better communicated and simplified for the general public?

1.2.1 Overlay Matrix

Table 1. Matrix Overlay

Investigative Question	Theorical Framework	Research Methods	Interview / Survey Question	Results
IQ1. How does the public perceive and interact with privacy laws in Switzerland?	GDPR, FADP and Their Public Understanding Society and Privacy in the Digital Era Digital literacy in Switzerland	Survey Expert interviews	Survey: Q5, Q7 Interviews: Q4-Q8	Insights into the public's understanding, misconceptions, and engagement with privacy laws.
IQ2. What societal impacts do privacy laws have on citizens' daily lives and their trust in institutions?	GDPR, FADP and Their Public Understanding Trust in Digital Systems	Survey Expert interviews	Survey : Q6, Q8, Q9, Q11, Q12, Q13, Q14 Interviews: Q3-Q6, Q9-Q13	Observations on behavioral changes, trust in digital systems, and privacy laws' effect on institutions and individuals.
IQ3. How can the complexity of privacy laws be better communicated and simplified for the general public?	GDPR, FADP and Their Public Understanding Privacy As a Right Digital literacy in Switzerland	Expert interviews Analysis based on the survey and the interviews	Survey: Q15 Interviews: Q14, Q15	Recommendations for improving public awareness and accessibility of privacy laws.
IQ4. How do privacy laws influence individuals' digital sovereignty and empowerment in Switzerland?	Digital Sovereignty Digital literacy in Switzerland	Expert interviews Survey	Survey: Q10, Q13	Better understanding of what is digital sovereignty its current state and ways to attain it fully.

1.3 Scope and limitations

This scope will be limited geographically to Switzerland but will use some insights from the rest of Europe as needed. Also, because most of the studies found in the social field are from around the world, and especially the United States of America, those will be used to draw comparisons.

For the purpose of a precise explanations of the complex concepts behind the thesis, the theoretical framework will not be limited geographically as it will make the research available sparse.

The empirical study is based on the data collected from Swiss citizens and two experts working in Switzerland. The survey will be sent to a broader range of people (students, professionals from various fields, old and/or young people).

While laws will be analyzed for the purpose of the thesis, the focus will be on the societal impact of those and not the intricacies of lawmaking and international law.

For that reason, this thesis will only recommend and propose changes in the social aspects. It will not attempt to invent or change laws.

2 Theoretical framework

2.1 Key concepts

2.1.1 Privacy

Privacy is by no means a new concern. It can be easy to associate it with technologies, but the concept itself, while slightly changed in practice overtime, predates the digital era and is relevant in both analog and digital contexts. An important text published in the Harvard Law Review in 1890 by Samuel D. Warren and Louis D. Brandeis, gives us some historical insight: In it, the authors emphasized the need for legal protections to safeguard what Judge Cooley described as the right "to be let alone.". This quote shows that even in the late 19th century, freedom and privacy were intimately linked. The text also highlights two concepts: the circulation of photographs and the intrusion of journalism into private life. Issues that are still relevant and important today. Another interesting fact of this review is the emphasis placed on the damage to mental health caused by a breach of privacy, a concern that resonates even more profoundly in the digital age. (Warren S. D. & Brandeis L. D., 1890).

But what is privacy It is difficult to define, because there are many definitions of it, and these definitions are even changing over time. Also, different cultures have different views on the subject. For the sake of this thesis, here is a simple definition that should be able to unite all the others: “privacy is one's ability to control information about oneself “(Bélanger F & Crossler R. E. 2011).

The impact digitalization has on privacy can be defined by what Floridi refers to as “Ontological friction”, which, simplified, means how easily the information is transmitted in a set location (“region of the infosphere”). To help with understanding of this concept, they draw a comparison with a house inhabited by 4 students, informational privacy is limited (or not) by the thickness of the walls and the will to privacy of the different roommates (e.g. open or closed doors, time spent together). (Floridi 2005)

2.1.2 Data Protection

Data protection refers to the mechanisms, policies, and laws created to protect personal information in an increasingly data-driven society. In today's interconnected world, almost every online

interaction contributes to a digital profile that captures a wide range of personal details, from social media activity and browsing history to online purchases and search behavior.

This aggregation of individual digital footprints, when structured in machine-readable formats and collected at scale, becomes what is commonly referred to as "Big Data”. What distinguishes big data from massive data sets are the 3Vs: Volume, refers to the size or amount of data being generated and stored, often measured in terabytes or petabytes, Velocity, describes the speed at which data is created, collected, and processed in real time or near real time and Variety which indicates the different forms of data, such as structured (e.g., databases), semi-structured (e.g., XML, JSON), and unstructured (e.g., videos/photos, social media posts). There are many uses for it, such as tracking and monitoring individuals, targeted marketing and/or research. Effective privacy mechanisms are critical to mitigating the risks inherent to Big Data by protecting against unauthorized access, data breaches, and exploitation of sensitive information. (Andrew J. & Baker M. 2021)

In Switzerland, data protection is governed by the FADP, which was created based on the European Union's GDPR. These laws define what is considered a lawful use of private and sensitive data, such as respect for individual rights, data protection, company transparency, risk mitigation, and crisis resolution (e.g., after a data breach). Another important component is the introduction of the DPO. The Data Protection Officer is a position in a company that oversees the use of data. While it is not mandatory for small businesses to have a DPO, large users of personal data, public bodies and authorities, and those using sensitive data could be fined if a DPO is not appointed. (Regulation (EU) 2016/679)

2.1.3 Digital Literacy

Digital literacy is the knowledge of digital tools. It is ability to find, use, communicate, and critically evaluate information. For any kind of knowledge, it is difficult to assess an individual’s level of understanding. However, with the fast evolution of technologies, it is clear how important digital literacy is. This means that society needs to be able to close the gap of knowledge between certain demographic groups. For example, each new generation grows alongside more complicated technologies of the digital age, while the oldest are left to understand it on their own. This does not mean that the youngest people are digitally literate, as it can be particularly difficult for children to

distinguish between a safe and a risky situation online. In addition, they are more likely to take in as factual what is fun rather than what is true. (Livingstone 2014)

2.1.4 Trust in Digital Systems

Trust is a complicated notion to explain as it involves human emotions as well as complex frameworks. For the purpose of the following explanation, here is a definition coined by Duranti and Rogers: “Trust has been defined in many ways, but at its core it involves acting without the knowledge needed to act” (Duranti & Rogers 2012).

In digital systems, trust is an important component of data protection. A good example of this is Microsoft Windows, when someone downloads a software from the web, multiple mechanisms are working together to protect the user. First the legal framework limits what you can or cannot find on the internet, but it lacks in control as it is hard to monitor everything. Then there is the Microsoft trust system, which verify the author and integrity of the file, and forces you to manually validate the execution of the program. Finally, the antivirus protects you from potential cyberthreats that could have passed the first filters. (Microsoft 2024).

The main problem with systems purely based on digital trust is how it can be bypassed. For the case of Windows, there are many cases of hacking and obfuscation. (Graeber s.a.). In “A Survey of Trust Management Systems for Online Social Communities Trust Modeling, Trust Inference and Attacks” Ruan Y. and Durresi A. analyze trust in a less technical way by investigating online social communities. In their paper, we understand better how different communities are interconnected and how trust inside of those groups can be breached (Ruan & Durresi 2016).

To conclude, trust in digital systems can be viewed in two main ways: Socially and Technologically. This means that digital consumers need to be wary of people as well as technologies which makes it hard to trust anything online. This also means a need for better rights and transparency as the GDPR and FADP try to realize. (Williams, Hassandoust & Zhang 2020)

2.1.5 Digital Sovereignty and Governance

Sovereignty is a confusing term, even in academic circles, but the consensus is the close link between sovereignty and authority (Philpott 1995). As Philpott cites Robert Wolff, authority is “the right to command and correlatively, the right to be obeyed” (Wolff 1970).

Among academics there are many perspectives of what digital sovereignty is, but this concept will be deepened later in the thesis. For a good fundamental definition Falkner, Heidebrecht, Obendiek and Seidl write in their paper “Digital sovereignty” – Rhetoric and reality” (Falkner, Heidebrecht, Obendiek, Seidl 2024):

> The core of digital sovereignty stipulates the need for control of the digital on the physical layer (resources, infrastructures, devices), the code layer (standards, rules, design) and the information layer (content, data) (Chander A., Sun H., 2021; Floridi, 2020; Sheikh, 2022).

Academics have used different terms to demonstrate different viewpoints, such as data sovereignty, technological sovereignty cyberspace sovereignty, but no consensus has truly been found. (Couture & Toupin 2019).

2.2 Privacy As a Right

To understand privacy as a fundamental right, we will draw insights from the historical, philosophical, sociological and juridical fields. This will help better understand how those rights were shaped to become what they are now in the digital age.

First, what is a fundamental right and how does it differ from human rights. The difference lies in their universality. While a fundamental right is generally defined by a country’s constitution and protected by said country’s legal system, human rights are inherent to every human being. No matter where they live, where they were born, or what makes them who they are. In that regard, fundamental rights could be considered a culturally specific extension of human rights. (European union agency for fundamental rights 2013)

The United Nations protect privacy in the Universal Declaration of Human rights article 14, written in 1948: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection

of the law against such interference or attacks." (United Nations 1948). As said previously this predates the digital age and does not answer how it is protected nowadays.

What makes privacy a right? To answer this question, I would like to go away from a legal perspective and try to better understand this concept. In "On Human Dignity as a Foundation for the Right to Privacy", Floridi picks up the term human dignity from the GDPR and asks a similar question to mine. In their work, she argues that privacy should be protected as a part of self and not as a property: "'my' in 'my data' is not the same 'my' as in 'my car', it is the same 'my' as in 'my hand', because personal information plays a constitutive role of who I am and can become.". (Floridi 2016). From this perspective, data protection becomes inseparable from the protection of personal identity, autonomy, and human dignity. It reframes privacy not as a transactional asset to be managed or traded, but as a vital element of personhood. Therefore, defending privacy is not simply about regulating access to information. It is about safeguarding the conditions for individual flourishing, agency, and self-realization in a digital society.

2.3 GDPR, FADP and Their Public Understanding

In 2016, the General Data Protection Regulation (GDPR) was introduced to enhance the protection of EU citizens' personal data, applying to organizations both within and outside the European Union. Due to the complexity of the regulation and the broader subject of data protection, compliance, which became mandatory in 2018, can be particularly challenging for small and medium-sized enterprises. This section aims to unpack this complexity from both the organizational and individual perspectives. While the Swiss Federal Act on Data Protection (FADP) introduced its updated compliance requirements more recently, in 2023, the primary focus here will remain on the GDPR, as the FADP closely aligns with it in structure and intent. Notable differences, particularly regarding terminology and fine structures, will still be highlighted where relevant.

First, let's explain what the GDPR is about. Personal data is any information that could be identified, while sensitive data is data that should not be disclosed (e.g. Religion, health, etc.). The regulation tries to protect those based on seven principles summarized in the gdpr.eu website from article 5.1-2 of the GDPR: "

- Lawfulness, fairness and transparency: Processing must be lawful, fair, and transparent to the data subject.

- Purpose limitation: You must process data for the legitimate purposes specified explicitly to the data subject when you collected it.
- Data minimization: You should collect and process only as much data as absolutely necessary for the purposes specified.
- Accuracy: You must keep personal data accurate and up to date.
- Storage limitation: You may only store personally identifying data for as long as necessary for the specified purpose.
- Integrity and confidentiality: Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
- Accountability: The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles."

(gdpr.eu)

Technological means of protection are not defined by the GDPR but impose appropriate measures. This means that any failure to respect the above principles would be contrary to the regulation. If everything is respected a data breach is not necessarily unlawful but must be publicly informed in less than 72 hours.

Privacy by design means that data protection measures must be integrated into the development of systems and services from the outset, rather than being added later. Privacy by default ensures that personal data is automatically protected in any system or service without requiring the user to act. In practice, this means that only the minimum necessary data should be collected and processed by default settings. A common example is newsletter subscriptions: under GDPR-compliant design, the "subscribe to newsletter" checkbox must be left unchecked unless the user actively opts in. The same principle applies to the use of cookies, where non-essential cookies (e.g., for marketing or tracking) must not be enabled unless the user gives explicit consent.

To help institutional compliance, the EU provided some important tools. First, the introduction of the Data Protection Officer (DPO) role as we briefly talked about earlier. This new position gives company professional insight on how it should treat data in a legal and ethical manner. While the organization stays liable for any breach of the law, the DPO is a real asset to any trustworthy

company (European Data Protection Supervisor 2025). The FADP also introduce the PFPDT which is close to a DPO's function but at a cantonal level.

Finally, in both the FAPD and GDPR, data can be stored and transferred only to appropriate countries, the US being one of the unauthorized places. There was an agreement between the US and the EU called privacy shield and before that safe harbor. Both those were invalidated by Schrems II and Schrems lawsuits. Those lawsuits highlighted grave problems related to data protection in the US. (Tracol 2020)

2.4 Technological Ways of Protecting Data

In Swiss law, there are 8 typical infractions that should be known and monitored to better protect data. Translated from Dessislava 2023 Haute école de Gestion de Genève (HESGE) course :

- Personal data theft
- Undue access to a computer system
- Provision of information enabling unauthorized access to a computer system
- Deterioration of data
- Provision of information enabling the deterioration of data
- Fraudulent use of a computer system
- Fraudulent obtaining of a service
- Identity theft

(Dessislava 2023)

These typical infractions give insight on the potential breaches but not on the actual protection. Combined with the seven principles highlighted in the GDPR, cybersecurity can help mitigate threats to data privacy. Institutions rely on a range of technological and organizational solutions to protect data against cyber threats, unauthorized access, and breaches. Among these, cryptographic techniques, blockchain technology, privacy by design principles, and regulatory frameworks such as GDPR and ISO 27001 play key roles in mitigating risks and ensuring compliance.

Cryptography serves as a foundational technology for data security, using encryption to protect information both in transit and at rest. Strong cryptographic methods, including advanced encryption standard (AES) and homomorphic encryption, ensure confidentiality while allowing secure

computations on encrypted data (Rawat, Doku & Garuba 2021). Hashing functions, digital signatures, and public-key infrastructures (PKI) strengthen authentication, authorization and data integrity, preventing unauthorized modifications (Rawat et Al. 2022). However, by themselves those technologies, as any other, can be bypassed. For example, digital signatures can be obfuscated by either technological means (Graeber s.a.) or human failures, as in the MSI key leak in 2023 (Goodin May 2023)

Artificial intelligence and machine learning enhance data protection by enabling predictive threat detection and anomaly detection. These technologies process enormous amounts of data in real-time, identifying changes from normal behavior and signaling potential cybersecurity threats. AI-driven intrusion detection systems (IDS) and security information and event management (SIEM) tools integrate big data analytics to analyze security logs and mitigate attacks efficiently (Rawat, Doku & Garuba 2021). However, adversarial machine learning presents a new risk, as cybercriminals started exploiting AI weaknesses to evade detection, necessitating ongoing research into AI security mechanisms (Rawat et Al. 2022). This demonstrate again that no technologies are safe from threats. Also, a less documented ethical and legal problem is the infringement to privacy and copyrights in the training of efficient AI models. (Lucchi 2024)

In addition to the above, blockchain technology, while new, offers an interesting layer of security through decentralization and cryptographic validation. Distributed ledger technology (DLT) ensures data integrity by recording transactions in immutable, tamper-proof blocks. This approach reduces reliance on centralized authorities, mitigating risks associated with single points of failure. Smart contracts further enhance security by automating rule-based transactions, reducing human intervention and associated vulnerabilities. However, blockchain-based systems must navigate regulatory challenges, particularly in complying with privacy regulations such as GDPR’s right to erasure, which conflicts with blockchain’s immutable nature (Rawat et Al. 2022).

The concept of Privacy by Design emphasizes integrating data protection measures into the development process of software and digital services. Rather than treating privacy as an afterthought, it ensures that security principles such as data minimization, user control, and transparency are embedded from the outset (Rubinstein & Good 2013). By implementing mechanisms such as default encryption, fine-grained access controls, and transparent data processing policies, organizations

can proactively safeguard user privacy. Worryingly, business incentives often compete with privacy concerns, requiring regulatory intervention to enforce compliance and accountability.

Regulatory frameworks such as GDPR and ISO 27001 provide legal and organizational guidelines for data protection. GDPR enforces strict controls over data collection, processing, and storage, emphasizing user consent and data subject rights. Organizations must conduct Data Protection Impact Assessments (DPIAs) to identify risks and implement appropriate safeguards. ISO 27001 complements GDPR by offering a structured approach to cybersecurity, incorporating risk management, incident response, and encryption protocols. (Rawat et Al. 2022)

The rapid expansion of IoT networks presents new challenges for data protection. IoT devices generate vast amounts of sensitive data, often with limited built-in security measures. As a result, IoT security relies on intrusion detection systems, anomaly-based monitoring, and automated threat response mechanisms. Big data analytics enhances IoT security by aggregating and analyzing data streams in real-time to identify suspicious activities (Rawat, Doku & Garuba 2021).

The GDPR itself encapsulates several key provisions that underscore the importance of technical and organizational measures in protecting personal data. Among these are the rights granted to individuals, such as access, rectification, and erasure of their data, which place significant responsibilities on data controllers and processors. The regulation mandates that organizations implement appropriate technical protection (including encryption and blockchain where applicable) and maintain robust internal processes (e.g., the appointment of a DPO) to ensure compliance. This regulatory framework not only enforces high standards for data protection but also incentivizes continuous innovation in technological defenses (Regulation (EU) 2016/679).

2.5 Digital literacy in Switzerland

As mentioned in the key concepts, digital literacy is not only about understanding and using digital tools, but also about having the critical thinking skills needed to navigate the digital infosphere. This means that children need to be educated as early as possible to ensure that they are mature enough to grow up safe. (Livingstone 2014)

In Switzerland, education is separated by language, which are French, German and Italian. Each of the 26 cantons must follow federal guidelines but are free to decide on the specifics of their education. (Swiss Confederation s.a.)

In the last 20 years, the growing importance of digital media has forced education professionals to improve Digital Media Learning (DML) in children's education. (CIIP s.a.) By comparing the curricula in the three main Swiss languages, we should be able to gain a better understanding of how digital literacy is defined, taught and assessed in Switzerland.

First, in the three curricula, DML is divided into 2 main disciplines, Information Technology and Media. The Italian curriculum has the most comprehensive yet simple definition: "To use digital technologies and media critically, creatively and consciously in order to actively create, learn and participate in society". (Translated from Piano di studio della scuola dell'obbligo)

For that purpose, the 3 study plans mention dividing in practical and theoretical education to help children develop critical thinking and ease of use at the same time. The French study plan explains this well by mentioning:

"Education to digital, by digital […]:

- The first enables students to develop a digital culture needed to understand a society where digital technology has become essential and to enroll in it as an active, creative and responsible citizen.
- The second offers multiple opportunities for students to understand disciplinary learning through activities, materials and tools tailored to their educational needs." (Translated from CIIP)

2.6 Digital Sovereignty

Digital sovereignty is mostly about control over digital infrastructures and data within the digital world. In recent years, both government and individuals have been trying to assert their digital sovereignty to fight against the increasing influences of multinational corporations and foreign governments. (Couture and Toupin 2019) This can be demonstrated, for example, by the US will to ban TikTok. (Clausius 2022)

2.6.1 Personal Sovereignty

At an individual level, digital sovereignty is the ability of users to control their personal data, make informed decisions about their digital interactions, and resist surveillance capitalism. (Zuboff 2019, Andrew & Baker 2021) Nowadays, big data allows corporations and governments to identify and profile individuals while influencing their online or even offline behavior. This highlights how crucial digital literacy is for personal digital sovereignty.

All of the different aspects we mentioned before, be it regulations (GDPR, FADP or others), digital literacy, and data protection technologies are necessary to empower the population in a growingly obscure digital space. (Sonnenberg & Hoffmann 2022, Farias-Gaytan Aguaded and Ramirez-Montoya 2023, Mehrnezhad Van Der Merwe and Catt 2024)

However, those measures do not totally erase the challenges that individuals have to face to ensure their sovereignty. Most digital services will have to trade between privacy for convenience, while legal and practical complexity of policies grows the gap even more. (Obar J.A. & Oeldorf-Hirsch 2020, Custers 2022)

2.6.2 Governmental sovereignty

Governmental sovereignty suggests that a state has the ability to regulate, secure and control digital infrastructures, data flows and digital policies within its realm. Many states seek to develop self-sufficient digital infrastructures to reduce dependence on foreign technologies and services to prevent data exploitation by external actors. As advocated by Macron (2017) and outlined by Falkner “sovereign Europe which would ‘lead rather than undergo the digital transformation’ by promoting its model within globalization, a model combining innovation and regulation” (Falkner *et al.* 2024). In the case of the European Union, the GDPR serves as an effort to claim regulatory power over data by implementing strict regulations on entities in its jurisdiction (Andrew & Baker 2021) and thus claims a form of sovereignty framed by Flonk, Jachtenfuchs and Obendiek as “Public order”, opposed to “Free access” in regards to governmental digital sovereignty. We will explain to these two framings later in this thesis. Similarly, Switzerland has strengthened its digital sovereignty through strict data protection regulations and a push for national cloud infrastructure to reduce reliance on non-European tech giants. However, Flonk, Jachtenfuchs and Obendiek argue that

regulatory efforts like the EU's digital sovereignty initiatives often conflict with global internet governance principles. This is shown by some states using the term digital sovereignty to restrict freedom of speech. (Falkner *et al.* 2024; Flonk, Jachtenfuchs & Obendiek 2024)

Switzerland used an interesting approach to assert its digital sovereignty. By localizing data, the federal government states that it is a cybersecurity necessity, yet the geopolitical use of this approach seems evident, (Fratini & Musiani 2024) asking important questions on cross-border collaboration and national surveillance and how to achieve a compromise between international innovation and national sovereignty.

Blockchain technologies could be an engaging alternative to current infrastructures by providing decentralized but transparent control over data and transaction. However, as discussed by academics, while this technology could improve transparency, accountability and self-governance, it renders difficult the implementation of norms and regulations by governments. (Al-Saqaf & Seidler 2017, Batubara, Ubacht & Janssen 2018)

2.6.3 Intersectional conflicts in sovereignty

Governmental and personal digital sovereignty are deeply intertwined. Governments have been trying to implement policies to protect their citizen's digital right, as shown by the GDPR and FADP, but this could lead to excessive control and surveillance (Hofmann 2024). Fratini and Musiani demonstrate this balance by separating governmental sovereignty in two frames, "Free access" and "Public order". (Fratini & Musiani 2024)

Table 2. Frames about content control.

Frame	Problem Definition	Prescriptions
Free Access	the restriction of free access to content is a threat to liberal democracy	Self-regulatory solutions, empowerment of individuals or specific groups, such as parents, with limited state intervention
Public Order	the public order and the public interest are under threat from internal and/or external forces	comprehensive public regulatory interventions to strengthen public control

Again, Flonk, Jachtenfuchs and Obendiek warn that certain sovereignty measures, such as increased content control on the internet, risk infringing upon digital freedoms and individual autonomy. (Flonk et al. 2024)

Zuboff in The Age of Surveillance Capitalism argues that the erosion of digital sovereignty at the individual level is largely driven by corporate exploitation of personal data. She highlights how tech giants create predictive models of user behavior, effectively stripping individuals of autonomy over their digital identities. This commodification of personal data means that digital sovereignty is not only about national policies but also about resisting corporate surveillance and data extraction practices. The increasing integration of digital technologies into daily life has made it nearly impossible for individuals to completely opt out of data collection, further diminishing personal sovereignty. (Zuboff 2019)

The discussion of digital sovereignty is further complicated by transnational data flows and geopolitical dynamics. Countries must navigate between regulatory autonomy and participation in global digital governance frameworks (Kuner 2017). For example, the Schrems II decision by the European Court of Justice challenged the adequacy of US data protection standards, reshaping how data transfers between jurisdictions are regulated (Cate, Kuner, Lynskey, Millard & Svantesson 2017).

2.7 Society and Privacy in the Digital Era

Despite the growing significance of privacy in the digital age, research on the social impacts of its protection remains notably sparse. Existing studies tend to focus on highly specific contexts rather than providing a general examination of privacy issues. For instance, research on privacy concerns in the context of second-hand buying has shown certain consumer behaviors and attitudes and the gaps between the law and its knowledge by the population (Salehzadeh et al. 2024). Similarly, studies focused on the healthcare sector have revealed challenges in protecting patient data, highlighting both the potential for breaches and the necessity for absolute confidentiality (Bühler et al. 2024; Pletscher, Mändil & Glinz 2022). These investigations, while valuable in their respective domains, underscore a critical gap: the lack of integrated research that synthesizes findings across diverse contexts to form a comprehensive understanding of public perceptions and the societal implications of privacy laws.

In 2018, Obar and Oeldorf-Hirsch conducted an interesting research on how the population interacts with Terms of Services and Privacy Policies. In their study, they compare the gap between self-reported surveys and the actual facts of those interactions. To get factual data, they created a fake social media website and told participants that the goal of the study was simply to give feedback on it. In the Terms of Service, they added clauses that should be unagreeable if read. However, 97% accepted the Privacy Policy and 93% the Terms of Service. While the whole thing should have taken around 45 minutes to read, the study reports an average of 125 seconds spent reading both texts. Clickwraps, generally the popup that allows you to simply click I accept the terms of service, can be considered a major factor to facilitate the obscurantism around those legal texts, as the study shows that 74% of participants used them to accept the privacy policy. Unfortunately, the GDPR suggest that it is still an accepted practice. (Obar & Oeldorf-Hirsch 2020)

An additional area that warrants further exploration is the emerging field of FemTech—technologies dedicated to women's health. FemTech applications and devices collect extensive amounts of sensitive data, ranging from menstrual cycle tracking to fertility monitoring. The dual-use nature of such data, where it holds promise for personalized healthcare but also presents significant risks if misappropriated, has become a focal point for recent scholarly attention (Hofmann 2024; Mehrnezhad, Van Der Merwe & Catt 2024). These studies suggest that while FemTech can empower female users by providing critical health insights, it also exposes them to potential abuse if robust privacy safeguards are not enforced. Consequently, the intersection of FemTech and privacy laws represents a frontier in privacy research that is both underexplored and highly consequential.

3 Empirical Research

3.1 Research Approach

This study employs a mixed-methods approach; by combining qualitative interviews with professionals and quantitative survey data, the thesis aims to provide a comprehensive understanding on how privacy laws and digital sovereignty impacts the Swiss population. The quantitative survey aims to capture broad trends and a rather general perception, while the qualitative interview provides a deeper insight of the topic and an expert viewpoint.

By that combination, the study aims to bridge the gap between technical knowledge (interview) and statistical data (survey), offering a more comprehensive and richer perspective on the subject.

3.2 Quantitative Research

The survey was designed to gain a better comprehension on the Swiss population awareness, behavior and attitudes toward privacy and its legal aspect, digital sovereignty and trust in digital infrastructures. It consists of 15 questions that could be divided in 5 sections:

- **Demographics**: Age, gender, education level, and occupation to contextualize responses.
- **Awareness**: Understanding and/or knowledge of the GDPR and FADP and individual rights in digital systems.
- **Behavior**: Use of privacy related tools, reading privacy policies, and data protection habits.
- **Trust in institutions**: Confidence in governmental and corporate data protection efforts.
- **Digital Sovereignty Perspective**: Opinions on personal control over data, national data policies, and potential improvements to privacy protections.

The survey was distributed through my own contacts, while making sure different demographics were represented. The survey was sent to social studies students in parallel to Business students and IT students. It was also sent to a broader range of professionals from different fields and ages.

In conducting the survey for this thesis, no personally identifiable information was collected beyond general demographic data such as age, gender, and occupation. These demographic questions were included solely for analytical purposes to identify patterns within different respondent groups. All responses remain anonymous, and no data can be traced back to individual participants. The

survey was designed and administered in accordance with the principles of the General Data Protection Regulation (GDPR), ensuring transparency, data minimization, and the protection of respondent rights. Participation was voluntary, and all respondents were informed about the purpose of the research and their right to withdraw at any time. The collected data is stored securely and will be deleted upon the completion of the thesis project. Throughout the process, care has been taken to respect privacy and ensure that ethical standards of research and data handling are upheld.

3.3 Qualitative research

To complement the quantitative research, which is the main research method of this thesis, I conducted an Interview with two experts working in the data privacy field in Switzerland.

The interview followed an open-ended format, allowing respondents to elaborate on:

- Their understanding and experience with data protection laws.
- The perceived effectiveness of regulations like the FADP and GDPR.
- Personal and institutional barriers to digital sovereignty.
- Recommendations for improving privacy awareness and policy implementation.

The interview was conducted via Microsoft Teams, recorded, transcribed, and subsequently analyzed by comparing its content with the findings from both the theoretical framework and the survey results. While the interview primarily serves as a qualitative research method aimed at deepening the understanding of the quantitative findings, it also provided valuable insights that may have retrospectively influenced the refinement of the theoretical framework.

4 Analysis

The survey, named Navigating Digital Autonomy: Trust, Privacy, and Sovereignty in a Connected Society, was filled by 107 respondents. The demographics are as follows:

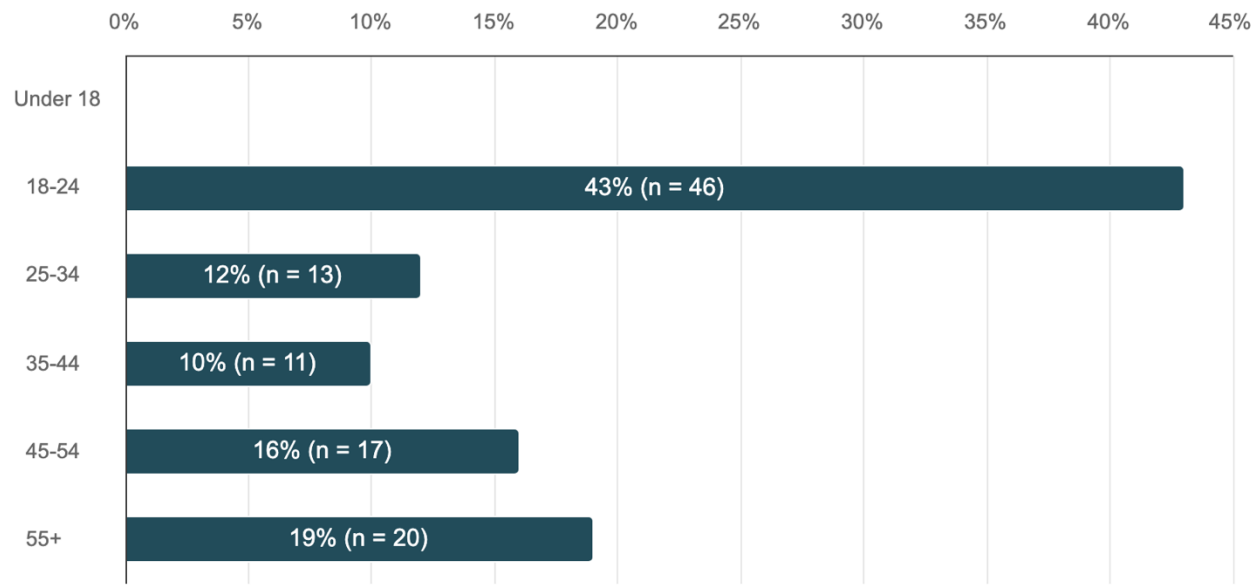


Figure 1. Age population

As we can see, the age range is skewed toward 18 to 24 years old and lacks people in the 25 to 44 years old demographic. This said, the sample size is sufficient to get a good idea of the difference between the younger and the older generation while having enough respondents in between to give a better perspective on the results.

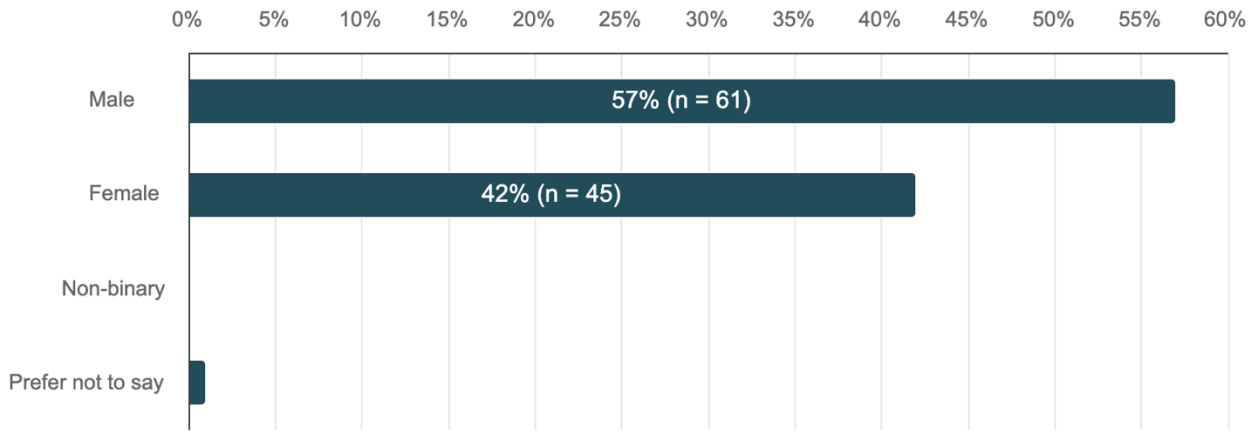


Figure 2. Gender

Unfortunately, the survey may be lacking a non-binary representation, but the male/female populations are quite even.

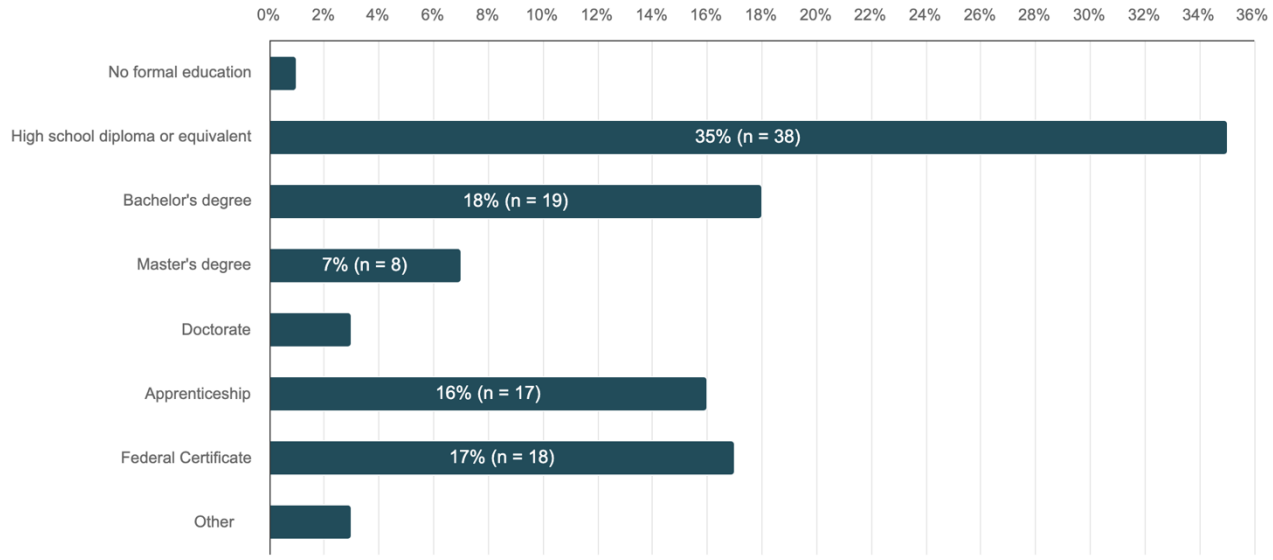


Figure 3. Education

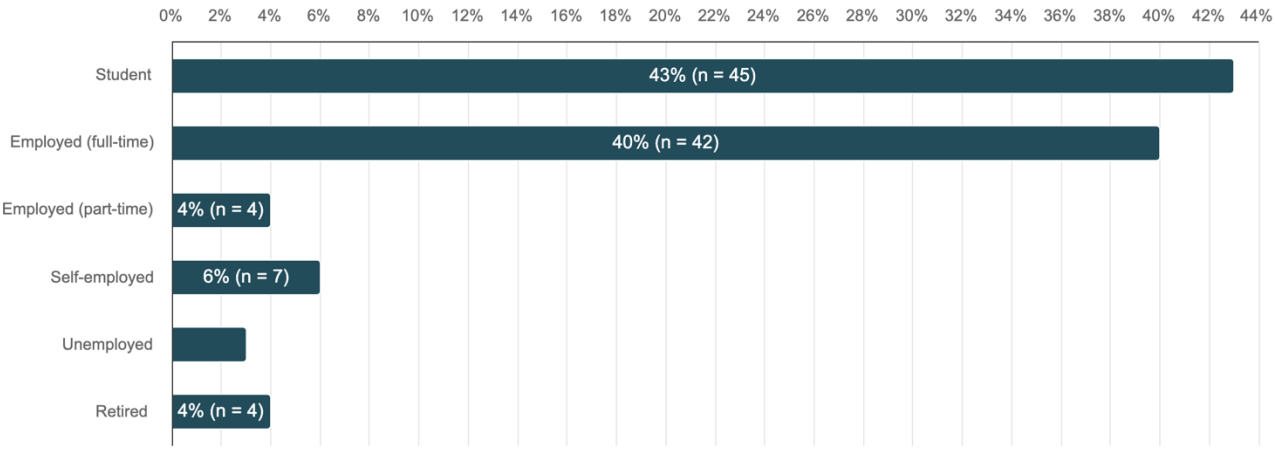


Figure 4. Occupation

In terms of education and occupation, the main fields are well represented. This should help us gain a better comprehension on the topic from most perspectives (different stages of life, lifestyle, etc.)

4.1 Descriptive Results

First, let’s go through every question’s data in their most basic form.

Table 3. Are you familiar with the Federal Act on Data Protection (FADP) and the General Regulation on Data Protection (GDPR)

Min value	Max value	Average	Median	Sum	Standard Deviation
0,0	10,0	5,6	6,0	410,0	3,0

88 people answered to that question, a value range of 0 to 10 and a standard deviation of 3 shows a wide array of different answers. While an average of 5.9 and a median of 6.0 seems to indicate that most people at least know of the FADP and GDPR.

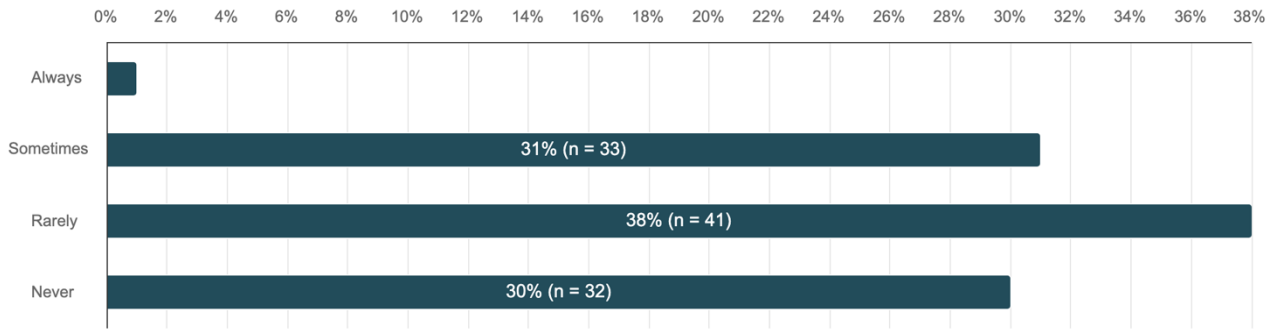


Figure 5. Do you ever read privacy policies before using an online service?

Here we see that only 1 of the 107 respondents always reads the privacy policies, while the other answers are relatively even. More than third (38%) only rarely read them and respectively 31% and 30% read them sometimes or never. The survey only shows what the respondents say and as Obar and Oeldorf-Hirsch demonstrate in “The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services”, the reality is often very different than what people may admit on that subject. (Obar and Oeldorf-Hirsch 2020)

Table 4. How well do you understand your digital rights under privacy laws?

Min value	Max value	Average	Median	Sum	Standard Deviation
0,0	10,0	4,7	5,0	359,0	2,6

Again we see a range between 0 and 10, although in this case 96 people responded. The average (4.7) and the median (5.0) are quite close with a standard deviation of 2.7.

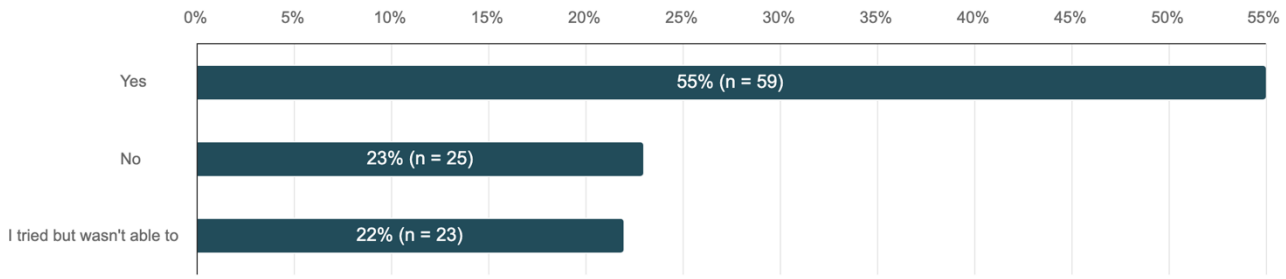


Figure 6. Have you ever changed your online behavior due to privacy concerns?

Out of the 107 respondents, a majority of people (55%) indicate having changed their behavior, while the rest have either made no change or at least tried (respectively 23% and 22%).

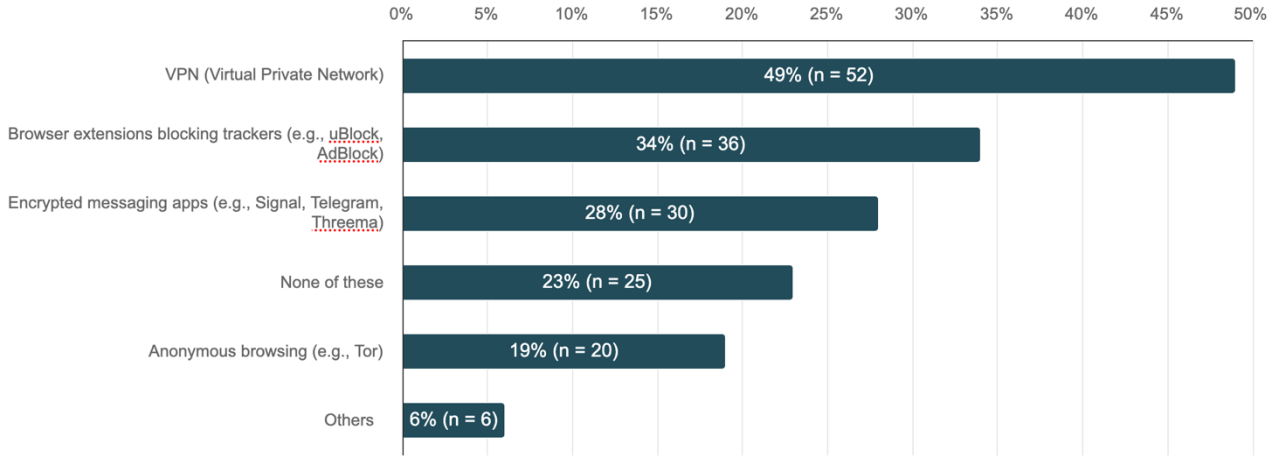


Figure 7. Which of the following privacy-enhancing tools do you use regularly? (Multiple choices)

Here the 107 respondents have selected 169 answers which means in average a respondent selected 1.58 answers. We can see that the choices correspond to the popularity of the tools, VPNs with 49%, ad blocking with 34% and encrypted messaging with 30%. Then 23% people used none of these and the less known anonymous browsers with 19%. Only 6 people indicate using other non-mentioned tools.

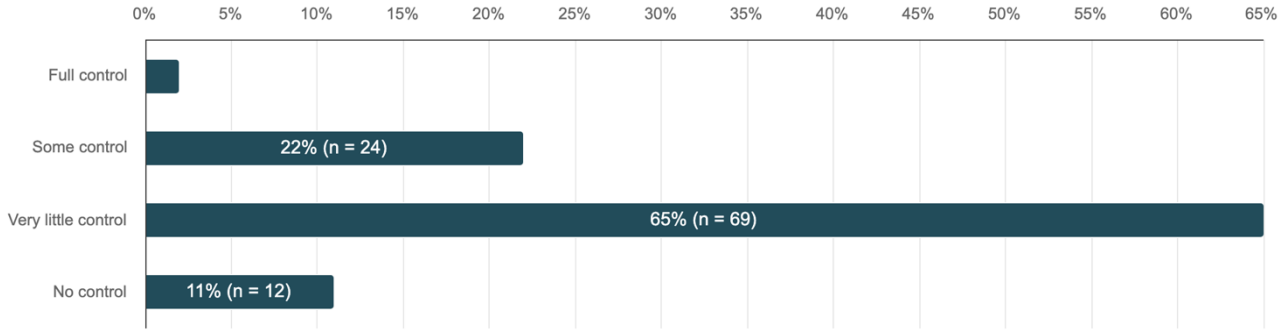


Figure 8. How much control do you feel you have over your personal data online?

Out of the 107 respondents a notable majority (69%) indicate having very little control over their personal data while only 2 of them consider having full control. Some control has been selected by 22% of the users and no control 11%.

Table 5. Do you trust the government to protect your digital privacy?

Min value	Max value	Average	Median	Sum	Standard Deviation
0,0	10,0	4,8	5,0	354,0	2,5

Here the scale is very similar to the previous 2. A range of 0 to 10, an average of 4.8 and a median of 5.0 with a standard deviation of 2.6 indicate, again, a wide range of different answers skewed toward the middle. For this question, 88 people responded.

Table 6. Do you trust large technology companies (Google, Meta, Amazon, etc.) to handle your personal data responsibly?

Min value	Max value	Average	Median	Sum	Standard Deviation
0,0	8,0	3,1	2,0	196,0	2,3

Here we also have a range from 0 to 10, however the average (3.2) and the median (2.0) are way lower than the other scale questions. This shows a lower perceived trust of private companies compared to governments. A standard deviation of 2.5 combined to the range also shows a rather high difference of answers between the 78 respondents.

Table 7. Do you think Switzerland should take stronger measures to protect digital sovereignty (e.g., developing national cloud services, reducing dependence on foreign tech companies)?

Min value	Max value	Average	Median	Sum	Standard Deviation
0,0	10,0	7,4	8,0	625,0	2,3

For this question, the range is again between 0 to 10 with a similar standard deviation (2.4). An average of 7.3 and a median of 8 shows that most people out of the 102 respondents strongly agree with stronger measures.

Table 8. In your opinion, does the Swiss government guarantee the protection of your private data?

Min value	Max value	Average	Median	Sum	Standard Deviation
0,0	10,0	4,6	5,0	395,0	2,1

Again the range goes from 0 to 10 with a standard deviation of 2.2. The average of 4.6 and the median of 5 seems to indicate that the 101 respondents are in between.

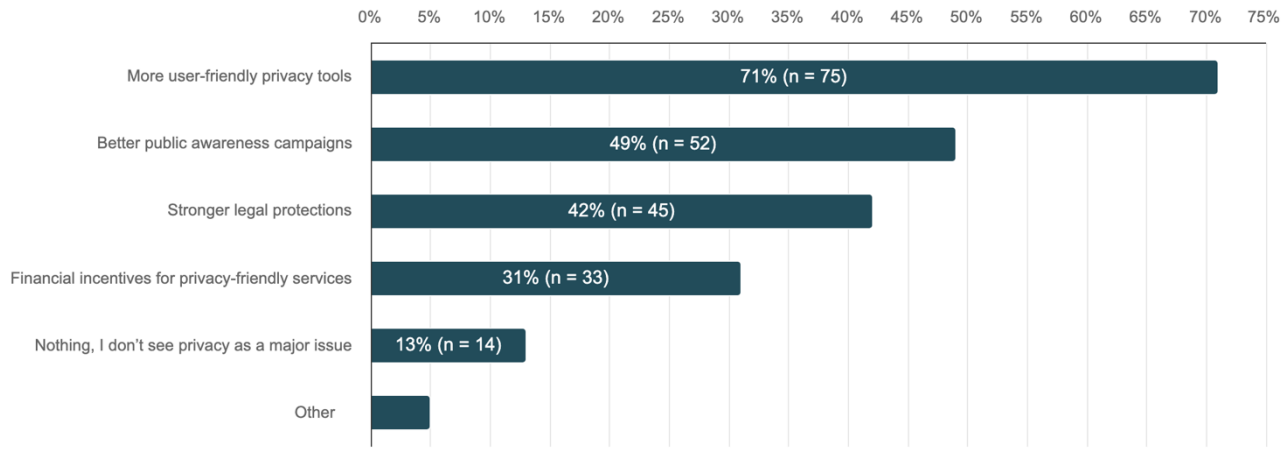


Figure 9. What would encourage you to take more control over your digital privacy? (Multiple choices)

Here, a 106 people answered with a total of 224 selected choices. This means that in average each respondent selected 2.11 answers. User-friendly tools come first with 71%, then better public awareness campaigns with 49%, stronger legal protections with 42% and financial incentives at 31%. Finally, 13% indicated not seeing privacy as a major issue and 5 people selected other.

4.2 Comparisons and Correlations

To be able to understand different groups of people, I decided to choose 3 comparison axes. The first is a simple age comparison:

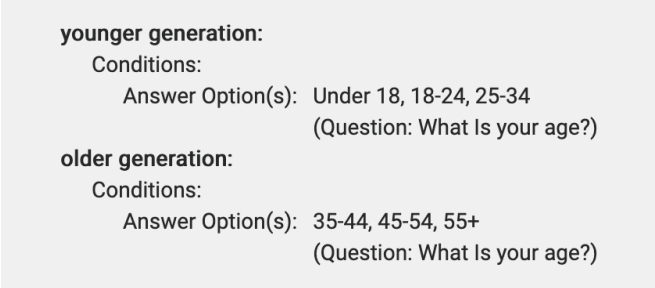


Figure 10. Age groups

The choice was made to take into account people that generally grew up with internet and technologies as we know them today against people that did not exactly. This will help to see in practice the differences in digital literacy among different generations. While 35 to 44 year olds are mostly familiar with technologies, the fast pace of change and the difference between early 2000 technology and 2020 justifies this choice.

The second axis is educational:

Figure 11. Education comparison

Professions with academic backgrounds and students speak for themselves, practicals are the people with a practical education and professionals with specific educations are those that did not go through the two majors education path in Switzerland. With this, we should be able to get a glimpse into digital literacy in the Swiss education system.

Finally a gender comparison will help us get an idea of the major differences of interactions in the digital sphere.

4.2.1 Age comparison

First let’s consider the demographical differences among age groups.

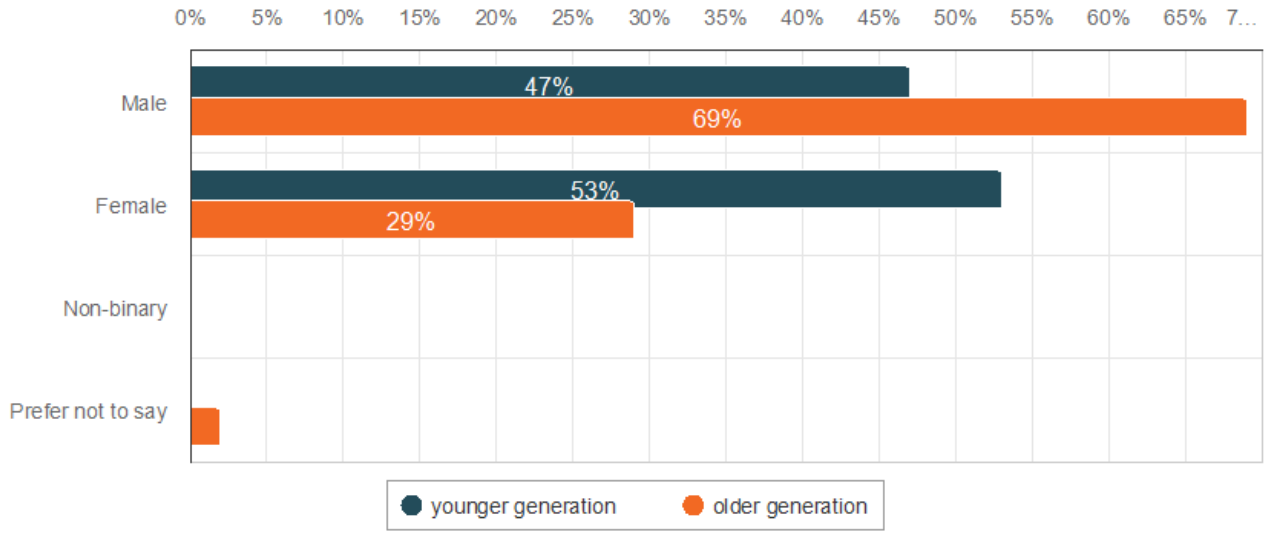


Figure 12. What is your gender?

Here we see that the younger generation has an almost even amount of men and women while the older generation is mostly men (69%).

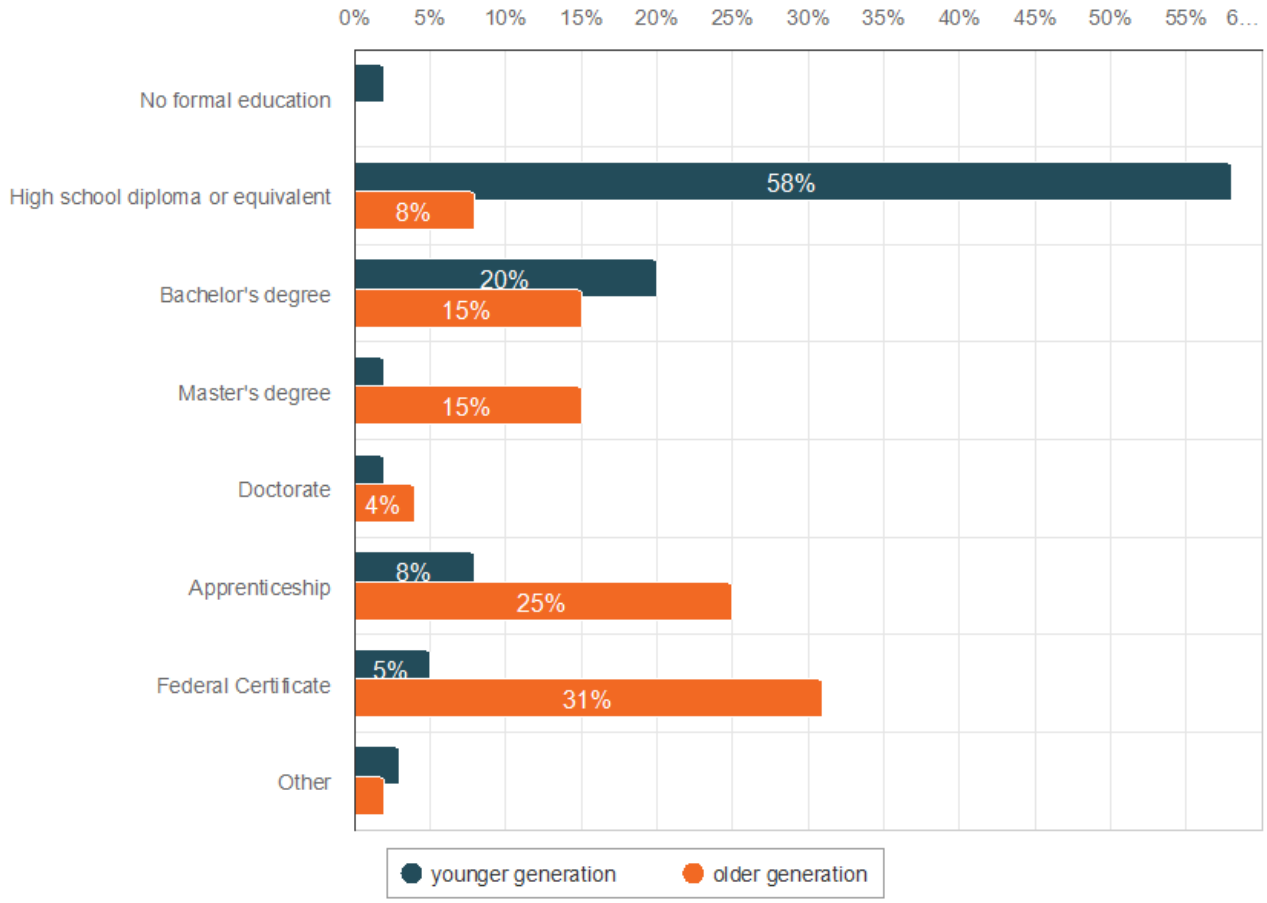


Figure 13. What is your highest level of education?

As expected, the younger generation is comprised of a majority of high school diplomas (58%) with 20% of bachelor degree's and a small percentage is distributed among the other categories.

The older generation is a bit more distributed. The highest percentages is the Federal Certificate with 31% and apprenticeship's with 25%.

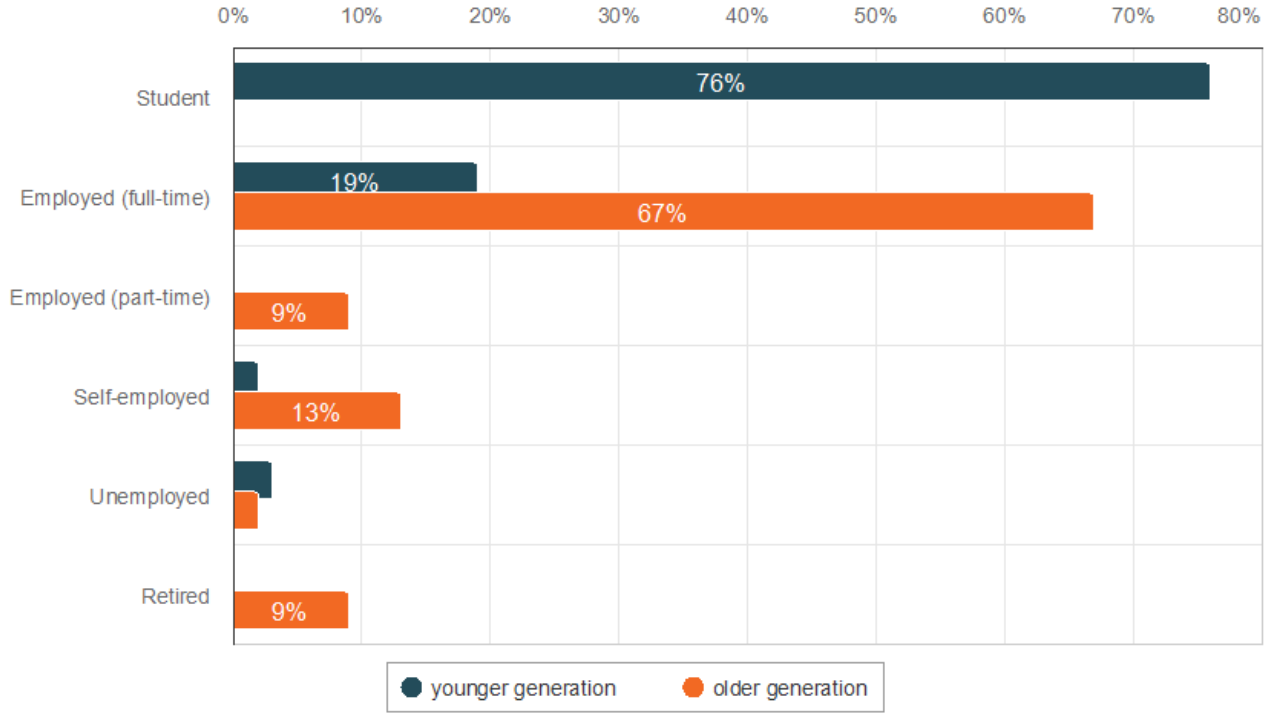


Figure 14. What is your primary occupation?

The last graph translates well into this one. We see that a vast majority of the younger generation (76%) are students. While the older generation is comprised of 67% of full-time employees.

Table 9. Are you familiar with the Federal Act on Data Protection (FADP) and the General Regulation on Data Protection (GDPR)

	n	Min value	Max value	Aver-age	Me-dian	Sum	Standard Devia-tion
younger genera-tion	43	0,0	10,0	4,3	4,0	183,0	2,8
older generation	45	0,0	10,0	7,4	8,0	332,0	2,3

The difference between the two group is vast. The younger generation seems to be significantly less familiar with legislation the older one. This is shown by an average of 4.3 and a median of 4.0 against 7.4 and 8.0. The question that is raised is if that can be explained by the fact that those legislation protects everyone but is enforced mostly at a business/company level rather than at a

personal level. This would mean that professional, which the older generation is mostly made of, are more confronted to the FADP and GDPR and would explain the statistical differences in knowledge of those.

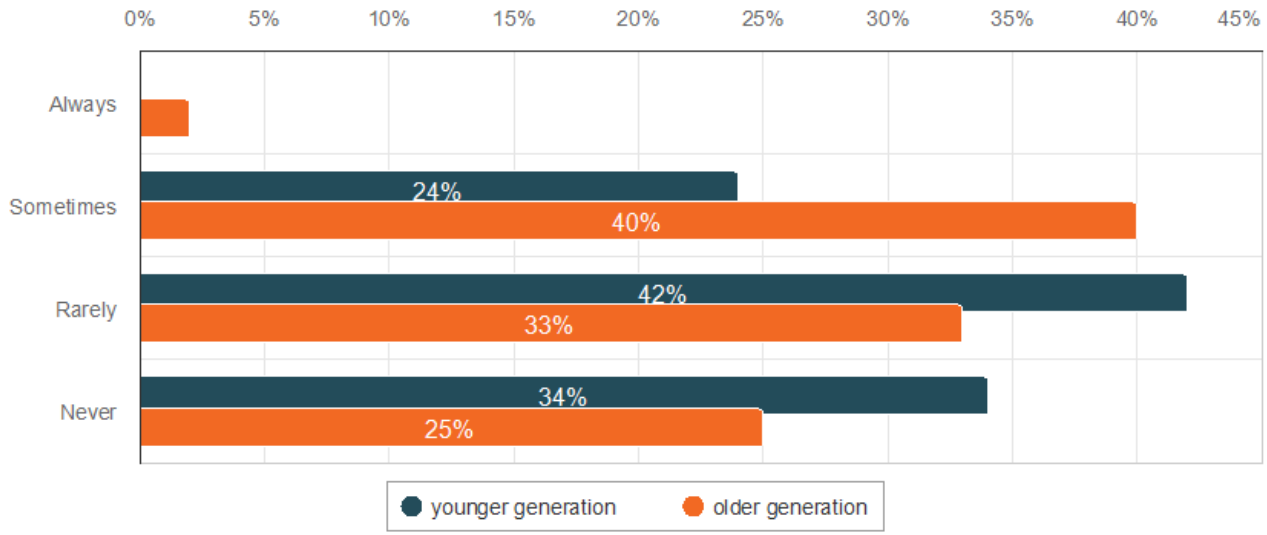


Figure 15. Do you ever read privacy policies before using an online service?

Here we see a tendency of the older adults to read the policies more than the younger population. 40% of the Senior respondents say the read them sometimes against only 24% for the Youngest's. While the difference is less notable, 42% against 33% for rarely and 34% against 25% for never confirms this tendency.

Table 10. How well do you understand your digital rights under privacy laws?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
younger generation	50	0,0	8,0	3,8	3,0	188,0	2,5
older generation	46	0,0	10,0	5,7	6,0	261,0	2,5

This table is closely linked to Table 3. As the older generation is more familiar with legislation, it is expected that they also understand their digital rights better than the younger one. As you can see the junior respondents has an average of 3.8 and a median of 3 with a maximum value of 8, while

the older population has an average of 5.7 and a median of 6 against a maximum value of 10. This shows again a clear gap in knowledge between the two populations.

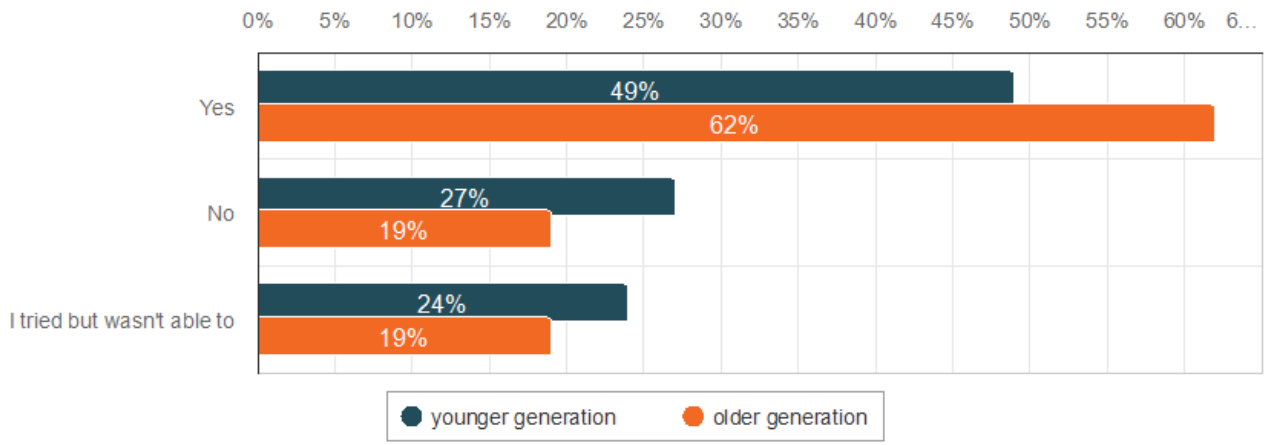


Figure 16. Have you ever changed your online behavior due to privacy concerns?

In this figure, we can see that older generation tends to change their behavior more than their younger homonyms with 62% of yes against 49%.

The difference here cannot be explained by legislative knowledge but may be by digital literacy. We can link this to section 2.1.3 of this thesis that explains, using Sonia's Livingstone's work, that while growing with technologies, children or even young adults, may not be able to fully realize the risk in the digital world. (Livingstone 2014)

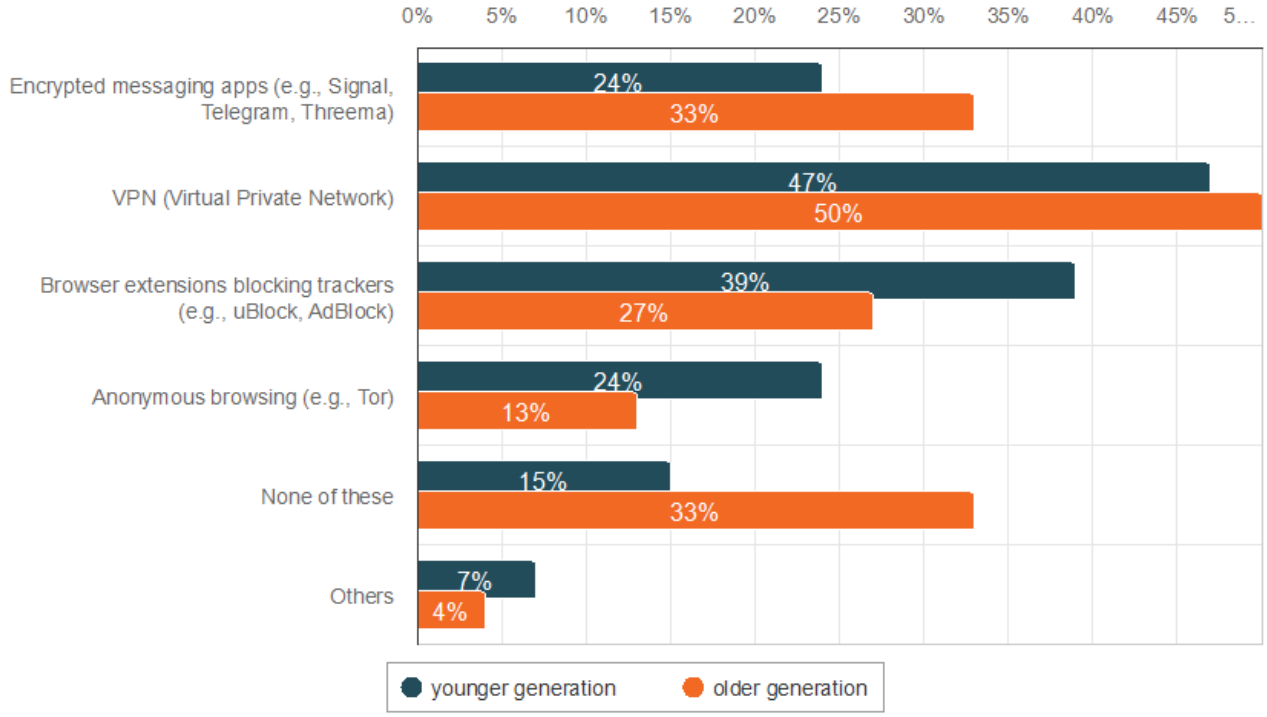


Figure 17. Which of the following privacy-enhancing tools do you use regularly? (Select all that apply)

We can see here some differences in the use of privacy-enhancing tools amongst the two groups the older generation seems to use encrypted messaging apps (33%) and neither of these (33%) more than the younger generation (24% and 15%). While the junior respondents indicate using browser extensions (39%) and anonymous browsers (24%) more than their seniors (27% and 13%). It is also important to note that the younger population selected more answers with 92 total answers against 77 for their senior. This could indicate that they use more tools in general.

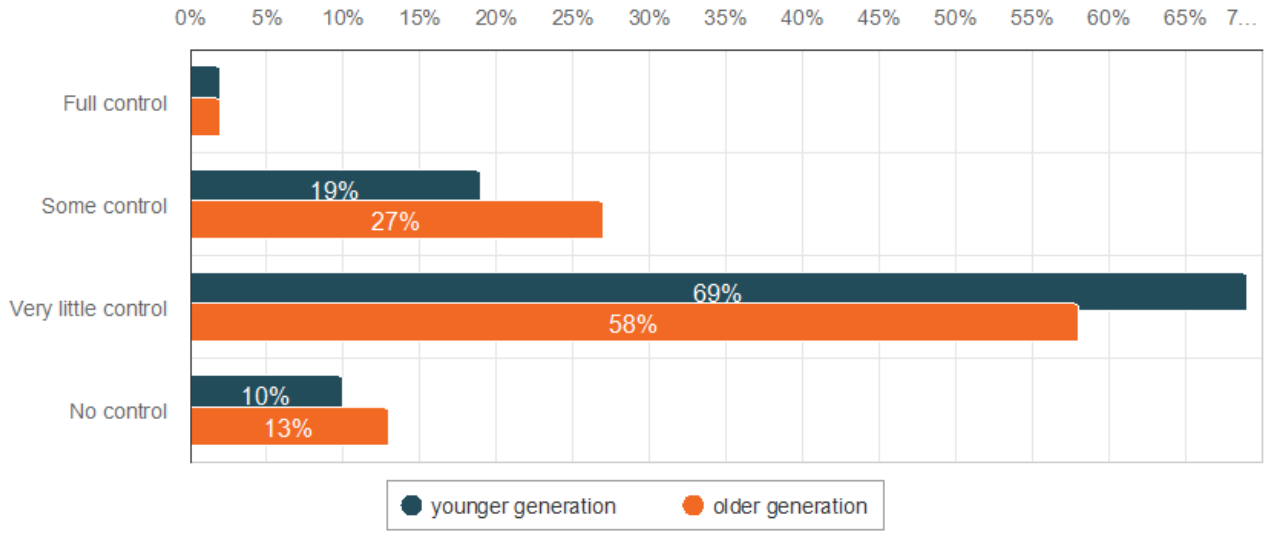


Figure 18. How much control do you feel you have over your personal data online?

Here the graph shows a small difference in the perceived control of data online. A big majority of the younger generation indicate feeling very little control (69%) while the older generation is at 58%.

Table 11. Do you trust the government to protect your digital privacy?

	n	Min value	Max value	Aver-age	Me-dian	Sum	Standard Devia-tion
younger genera-tion	50	0,0	10,0	4,6	5,0	229,0	2,6
older generation	38	1,0	10,0	5,0	5,0	189,0	2,6

Governmental trust is very similar in the two groups. That said the statistics seems to indicate little bit more trust of the older generation with a minimum value of 1.0 and an average 0.4 higher than their juniors.

Table 12. Do you trust large technology companies (Google, Meta, Amazon, etc.) to handle your personal data responsibly?

	n	Min value	Max value	Aver-age	Me-dian	Sum	Standard Devia-tion

younger generation	42	0,0	8,0	2,9	2,0	123,0	2,3
older generation	36	0,0	10,0	3,4	2,5	123,0	2,7

While similar, trust toward companies shows a noticeable gap between generations. This is demonstrated by a 2.0 difference in max value and a 0.5 in both average and mean values. The lower standard deviation seems to confirm a lower trust of the younger generation towards handling of data from big companies.

Table 13. Do you think Switzerland should take stronger measures to protect digital sovereignty (e.g., developing national cloud services, reducing dependence on foreign tech companies)?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
younger generation	55	0,0	10,0	6,9	7,0	379,0	2,4
older generation	47	1,0	10,0	7,8	8,0	368,0	2,4

Junior respondents seem to impose less responsibility on the Swiss government to protect digital sovereignty. This could be explained by the lesser trust hence the 0.9 and 1.0 lower average and median respectively.

Table 14. In your opinion, does the Swiss government guarantee the protection of your private data?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
younger generation	55	0,0	10,0	4,5	5,0	249,0	2,1
older generation	46	0,0	10,0	4,8	5,0	220,0	2,4

Here the values are almost the same except for a 0.3 lower deviation and average for the younger generation.

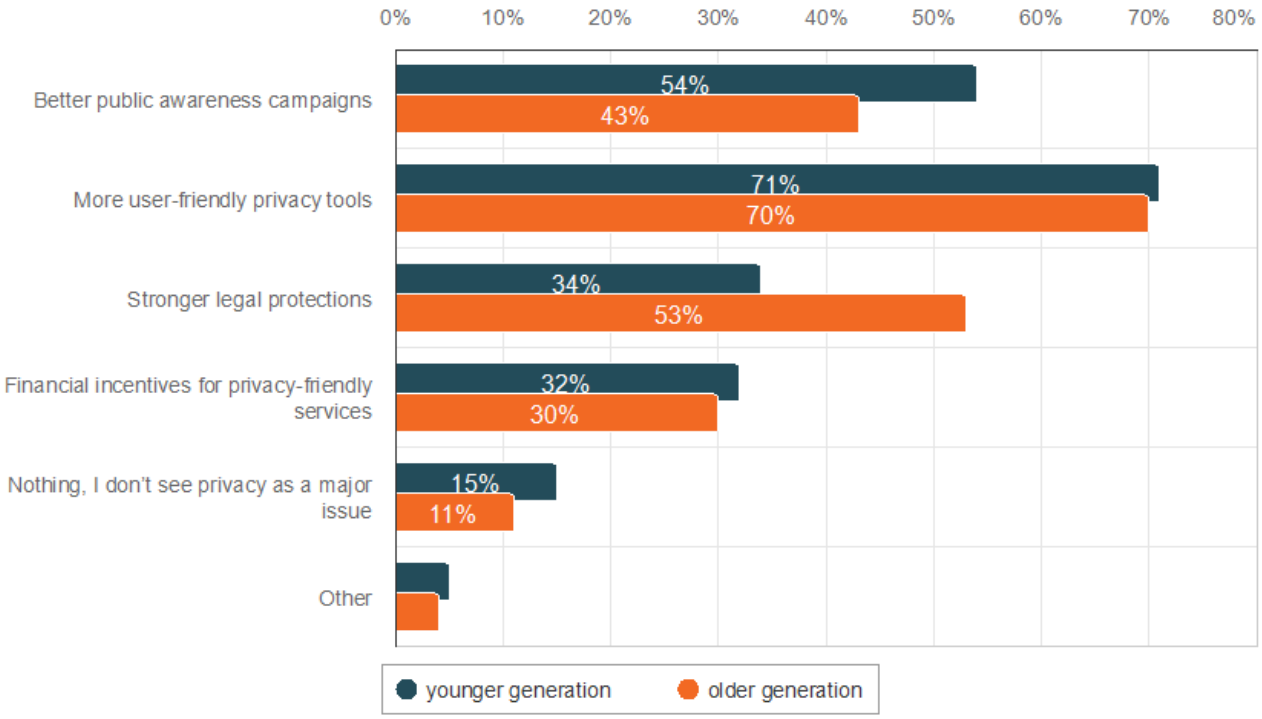


Figure 19. What would encourage you to take more control over your digital privacy? (Select all that apply)

The major difference shown is this graph is that 53% of the older generations encourage legal protections against 34% of their juniors, while 54% of the younger generation encourage better public awareness campaigns against 43% of their seniors.

4.2.2 Educational comparison

In this section, the population vary significatively in size. Especially the professional with specific education group which is comprised of less than 10 respondents. For that reason, I will only mention major differences and ignore the professional with specific education group except for some comparisons.

Table 15. Are you familiar with the Federal Act on Data Protection (FADP) and the General Regulation on Data Protection (GDPR)

	n	Min value	Max value	Aver-age	Me-dian	Sum	Standard De-viation
professionals with academic background	19	1,0	10,0	6,7	7,0	127,0	2,7
practicals	32	0,0	10,0	7,1	8,0	227,0	2,6
professionals with specific education	4	6,0	7,0	6,5	6,5	26,0	0,6
students	30	0,0	10,0	3,9	3,0	117,0	3,0

While most groups have relatively similar results, we see a far lower average and median in student's data. This can be linked to the age comparison as we know that most of the student pool are aged between 18 and 24.

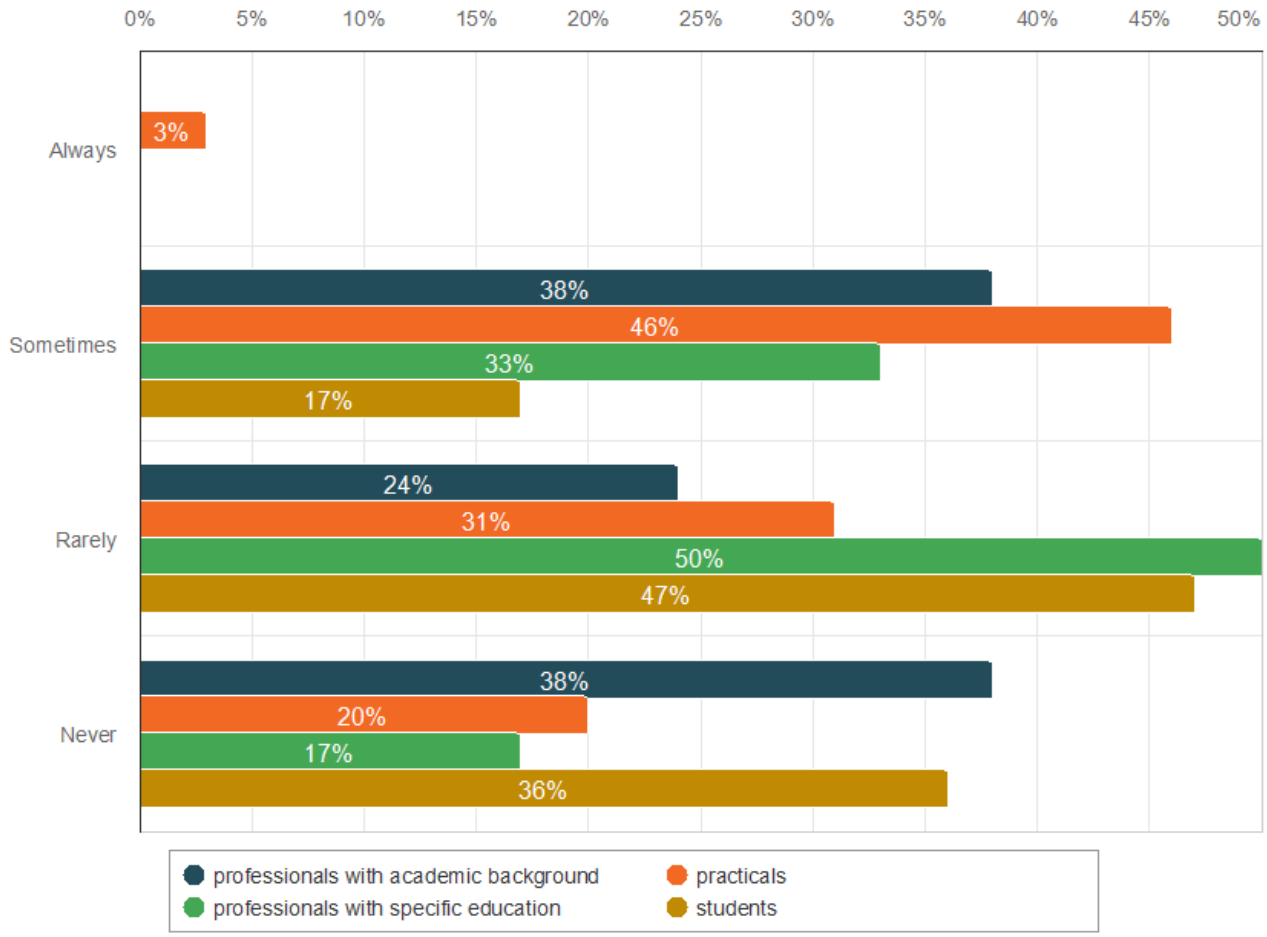


Figure 20. Do you ever read privacy policies before using an online service?

This graph shows that only 1 practical respondent answered always. Most of the students answered rarely (47%) then never (36%) and sometimes (17%). Practicals answered sometimes (46%) then rarely (31%) and never (20%).

Table 16. How well do you understand your digital rights under privacy laws?

	n	Min value	Max value	Aver-age	Me-dian	Sum	Standard De-viation
professionals with academic background	19	0,0	10,0	5,5	5,0	104,0	2,6
practicals	33	0,0	10,0	5,2	5,0	173,0	2,5
professionals with specific education	6	2,0	6,0	4,2	4,5	25,0	2,0
students	35	0,0	8,0	3,7	3,0	128,0	2,7

This, as it was for other comparisons, is related to legislative knowledge. Here we see again a lower average, max value and median in the student population.

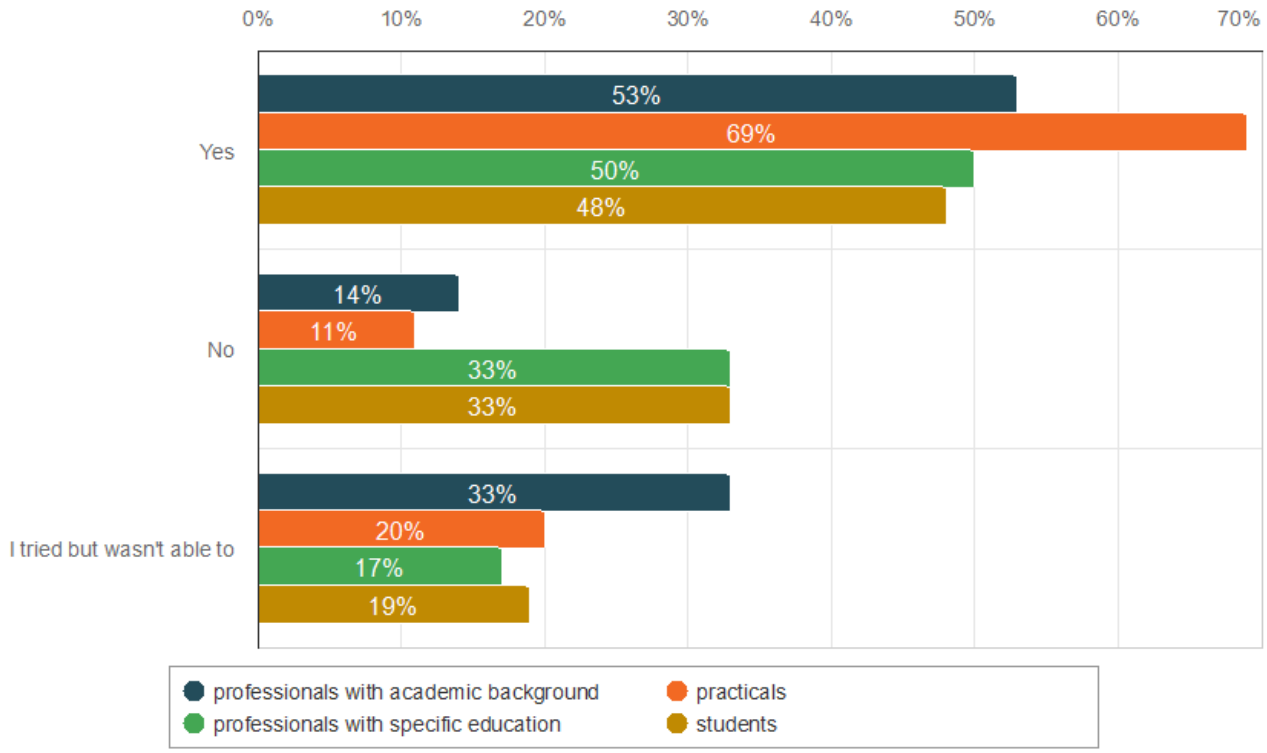


Figure 21. Have you ever changed your online behavior due to privacy concerns?

This graph shows that most groups answered mostly yes, and most notably the practicals with a 69%. This said, professionals answered (both 33%) no more than practicals and students. The

results for the “I tried but was not able to” option are very similar except for professionals with academic backgrounds with a 33%.

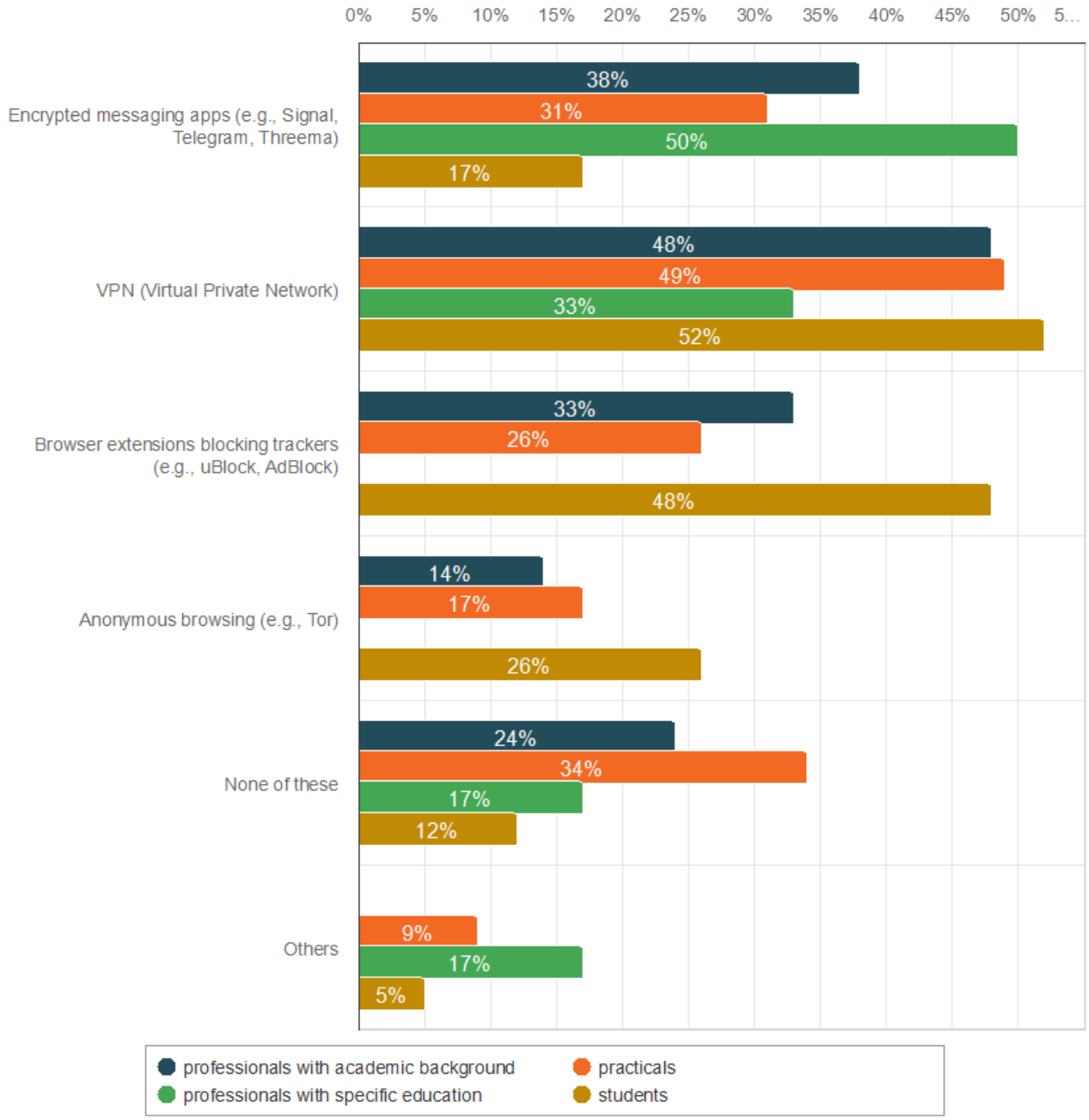


Figure 22. Which of the following privacy-enhancing tools do you use regularly? (Select all that apply)

Here we see different percentages but similar trends among groups. The notable differences is that students indicates using browser extensions and anonymous browsing more than the others. They also selected 40.3% of the total answers against 33.6% for practicals and 20.1% for professionals with academic background.

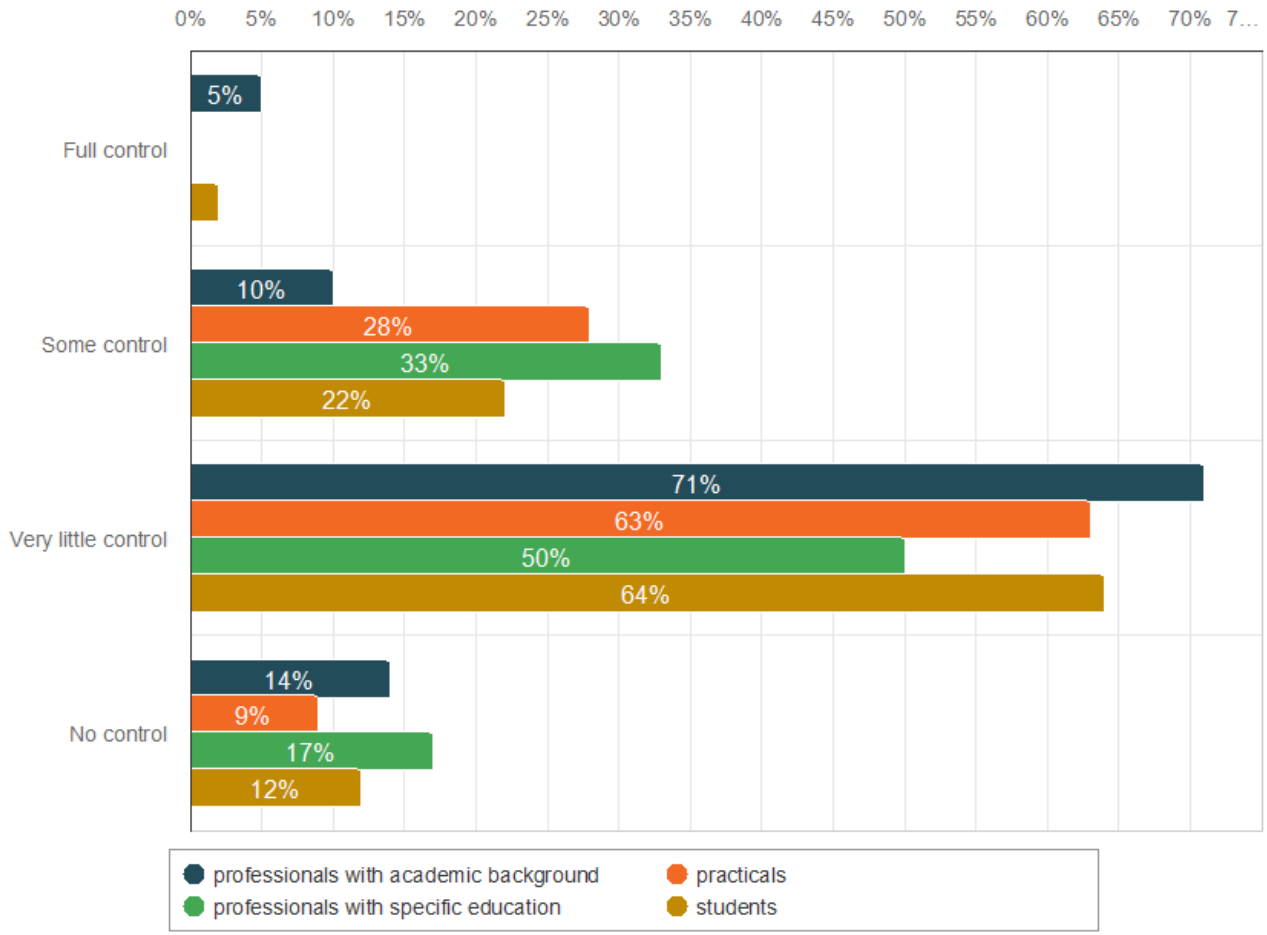


Figure 23. How much control do you feel you have over your personal data online?

We see again very similar trends, except for the professionals with academic whom only 10% answered “Some control” but answered “Very little control” more than the rest (71%).

Table 17. Do you trust the government to protect your digital privacy?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
professionals with academic background	15	0,0	10,0	4,9	5,0	74,0	2,6
practicals	28	1,0	10,0	4,6	4,5	128,0	2,3
professionals with specific education	3	1,0	2,0	1,3	1,0	4,0	0,6
students	39	0,0	10,0	4,9	5,0	191,0	2,7

Table 18. Do you trust large technology companies (Google, Meta, Amazon, etc.) to handle your personal data responsibly?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
professionals with academic background	14	0,0	8,0	2,4	2,0	33,0	2,4
practicals	25	1,0	10,0	3,8	3,0	95,0	2,8
professionals with specific education	4	0,0	2,0	1,3	1,5	5,0	1,0
students	32	0,0	8,0	3,0	2,5	97,0	2,3

Table 19. Do you think Switzerland should take stronger measures to protect digital sovereignty (e.g., developing national cloud services, reducing dependence on foreign tech companies)?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
professionals with academic background	21	3,0	10,0	8,6	10,0	180,0	2,1
practicals	32	1,0	10,0	7,3	8,0	233,0	2,6
professionals with specific education	6	5,0	10,0	8,7	10,0	52,0	2,2
students	40	0,0	10,0	6,6	6,0	263,0	2,3

There is similarities with the age comparison in this graph. We see again that students, who are mostly between 18 and 24 years old, have a lower average (6.6) and median (6.0) than the other groups.

Table 20. In your opinion, does the Swiss government guarantee the protection of your private data?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
professionals with academic background	20	0,0	8,0	4,1	5,0	81,0	2,1
practicals	32	0,0	10,0	5,0	5,0	159,0	2,5
professionals with specific education	6	1,0	5,0	3,8	4,0	23,0	1,5
students	40	0,0	10,0	4,8	5,0	191,0	2,1

The results are once again very similar, but we can see a lower max value (8.0) and average (4.1) amongst professionals with academic background than the rest.

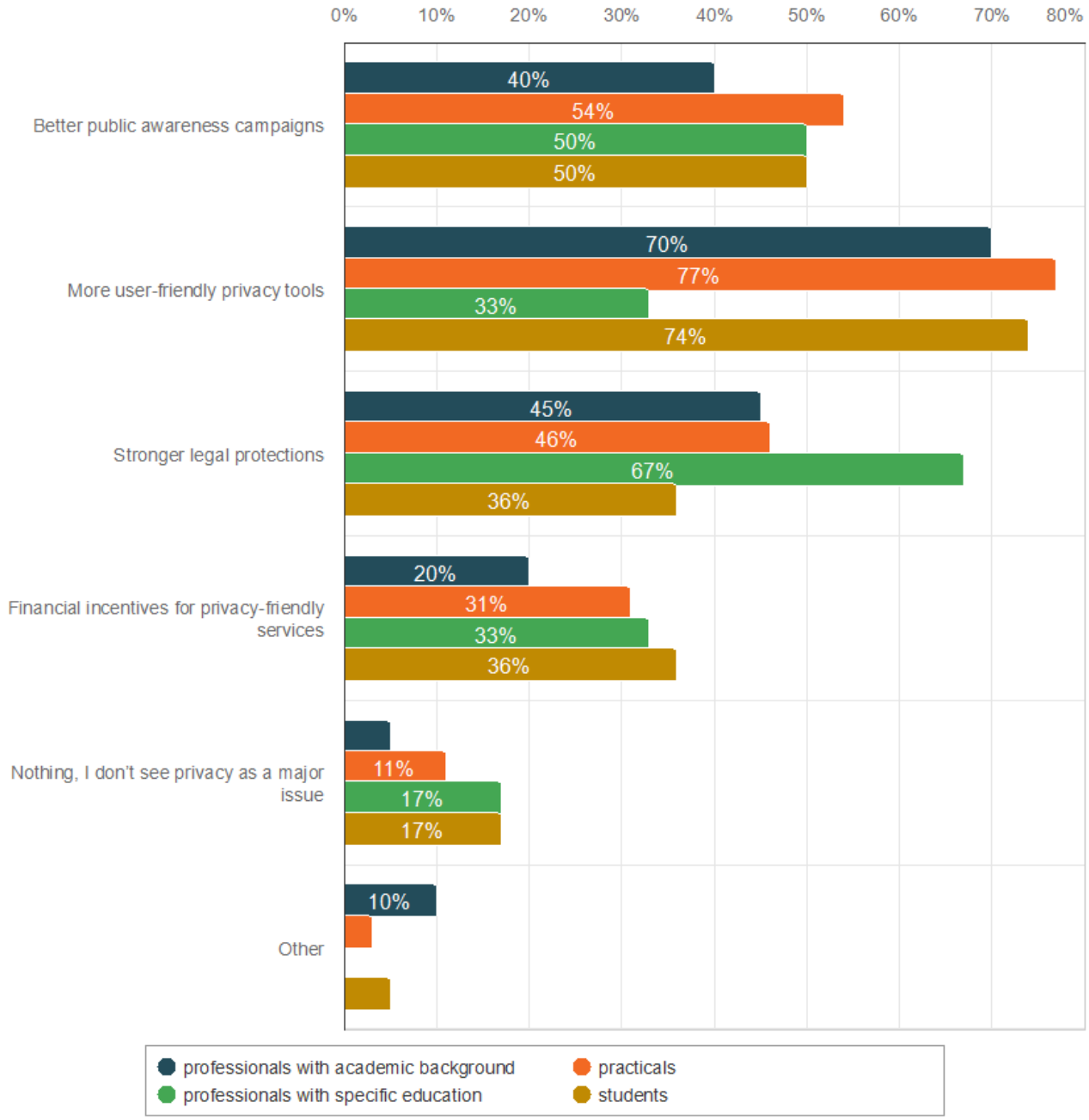


Figure 24. What would encourage you to take more control over your digital privacy? (Select all that apply)

In this final graph, we are seeing similar trends again. Although it is interesting to note that professionals with academic background have lower percentages in most options apart from the “other” one. That said they also have by far the lowest total answers with 38 while practicals have 78 and students 91.

4.2.3 Gender comparison

Unfortunately, the non-binary representation is only 1 percent so I decided to remove it from the comparison. Also, most of the data results are very similar between men and women. For that reason we will focus only on statistical differences.

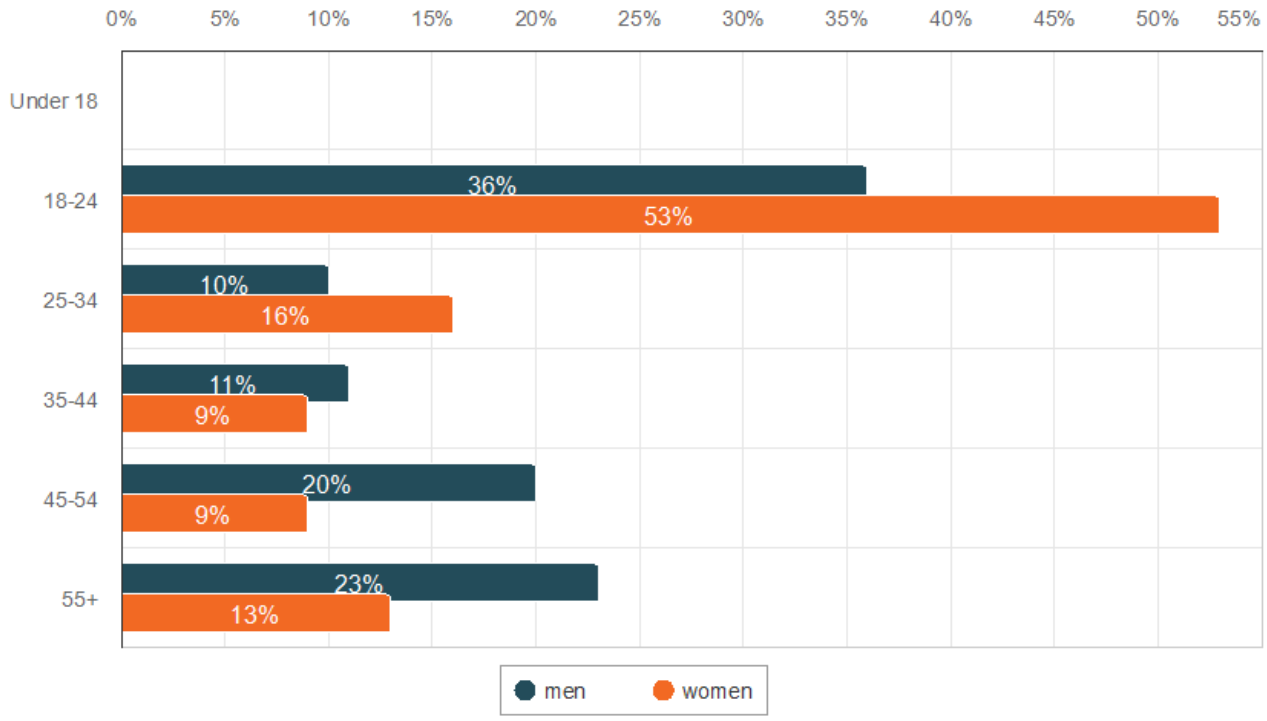


Figure 25. What Is your age? (Men – Women)

For the rest of this analysis, it is important to note that a majority of the female population (53%) is between 18 and 24 years old.

Table 21. Are you familiar with the Federal Act on Data Protection (FADP) and the General Regulation on Data Protection (GDPR)

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
men	49	0,0	10,0	6,4	7,0	313,0	2,9
women	38	0,0	10,0	5,3	5,0	202,0	2,9

The difference in familiarity with the FADP and GDPR between men and women is vast. A 1.1 difference in average and a 2.0 difference in the median indicate a lower familiarity of women. This explains and translates well into the next table.

Table 22. How well do you understand your digital rights under privacy laws?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
men	56	0,0	10,0	5,1	5,0	288,0	2,6
women	39	0,0	8,0	4,1	4,0	161,0	2,6

Here we can see a similar difference from the previous statistic.

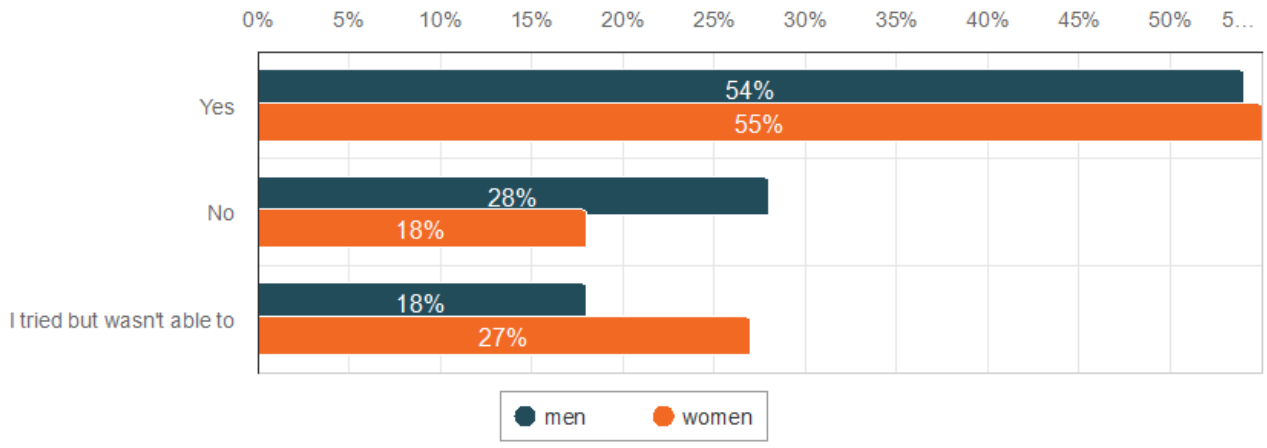


Figure 26. Have you ever changed your online behavior due to privacy concerns?

While a similar percentage indicate having changed their behavior, the graph shows that more women said trying but not be able to (27%) when men said they did not change anything (28%).

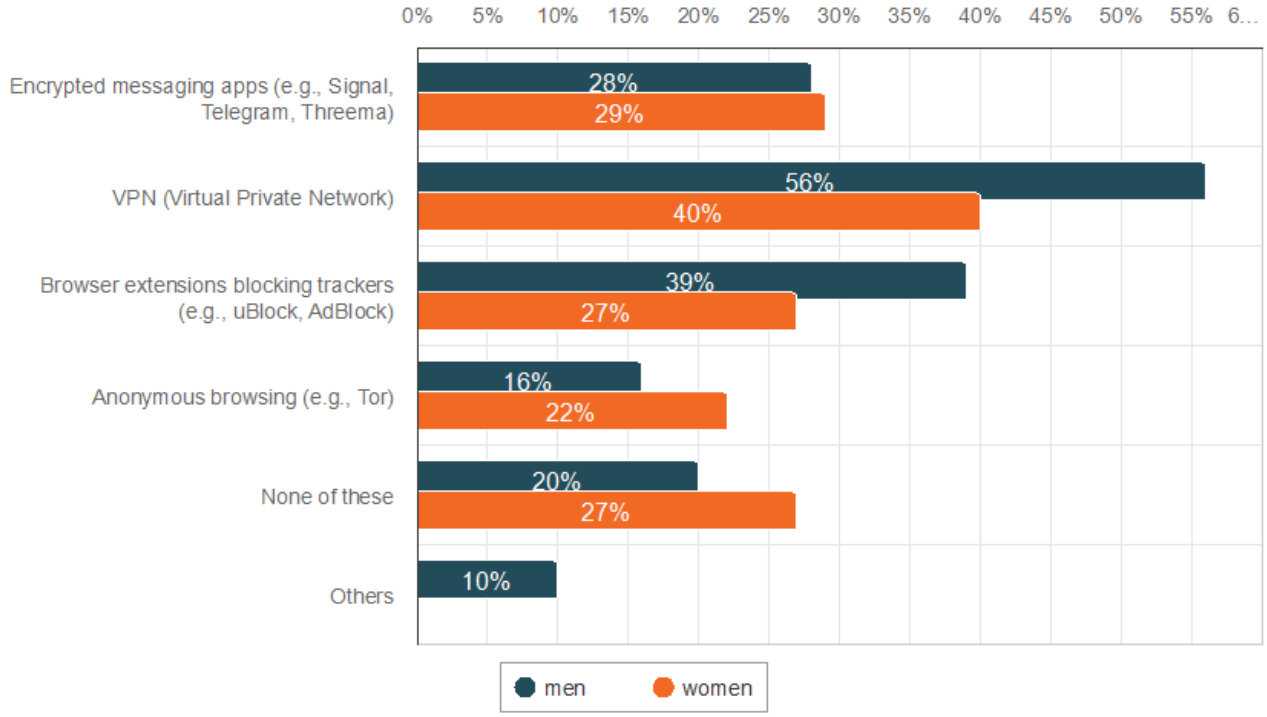


Figure 27. Which of the following privacy-enhancing tools do you use regularly? (Select all that apply)

This graph demonstrate that mean seems to use more tools than women. This is shown by a total of selected answers of 103 for men and 65 for women and by the fact that 7% more women than men have selected none of these.

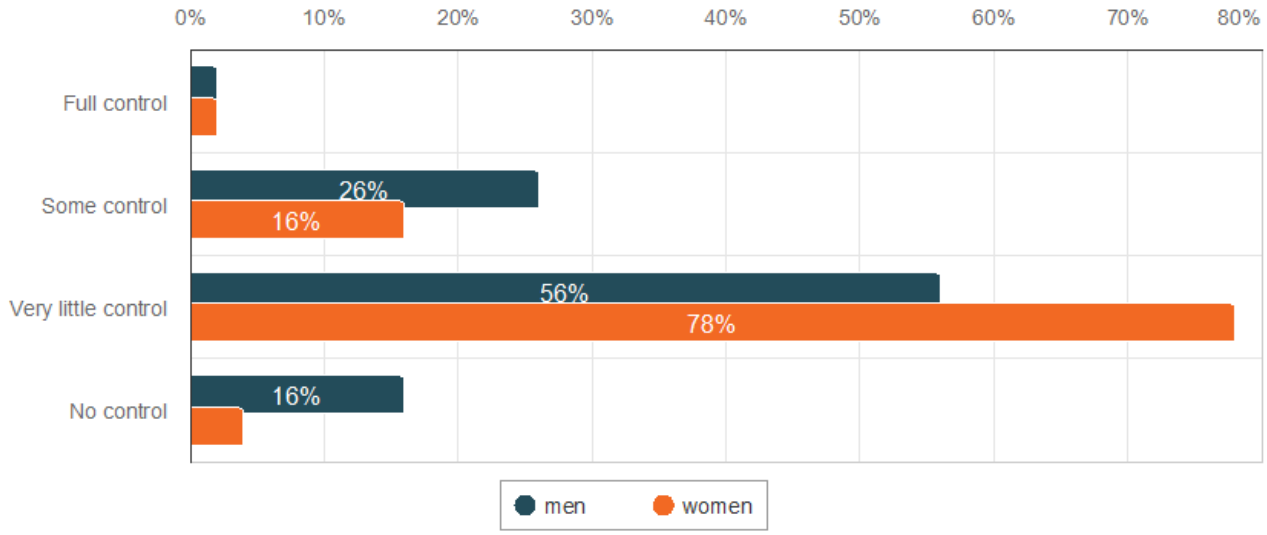


Figure 28. How much control do you feel you have over your personal data online?

Here a vast majority of women (78%) indicated having very little control over their personal data online and only 16% of them said having some control. 56% of men selected very little control while 26% of them indicated having some control. This could mean that women tend to feel less control online but this can be counter argumentized by the fact that 16% of men said having no control while only 4.4% of women said the same.

Table 23. Do you trust the government to protect your digital privacy?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
men	52	0,0	10,0	5,3	5,0	273,0	2,8
women	36	1,0	9,0	4,0	4,0	145,0	2,1

Table 24. Do you trust large technology companies (Google, Meta, Amazon, etc.) to handle your personal data responsibly?

	n	Min value	Max value	Average	Median	Sum	Standard Deviation
men	48	0,0	10,0	3,3	2,0	158,0	2,8
women	30	0,0	7,0	2,9	2,0	88,0	2,0

Both table 17 and 18 shows a similar thing. Trust among women be it for companies or governments tends to be lower. The max value, average and median tend to confirm this hypothesis. The lower standard deviation than in men's response also indicates a general lower sentiment and less differences in women's answers.

5 Discussion

The final chapter aims to conclude the work done throughout the thesis by reflecting on the key findings of both the quantitative and qualitative research and connecting them to the theoretical framework. Finally, I will offer proposals for improvements in the field of digital privacy awareness and sovereignty in Switzerland.

5.1 Interview summary and conclusion

The expert interview was conducted with an Information Security Officer at Bâloise Group, a major actor in the financial and insurance sector operating across Switzerland, Germany, Belgium, and Luxembourg. The conversation provided critical insights into the practical implementation of privacy laws, the challenges tied to compliance, and the broader societal implications of data governance in highly regulated industries.

5.1.1 Privacy Laws and the Financial Sector

In the financial world, data is treated as highly sensitive and its protection is paramount. According to the participant, privacy laws such as the GDPR and the Swiss Federal Act on Data Protection (FADP) are deeply embedded into the company's operations, particularly because of parallel regulatory frameworks like FINMA and the upcoming European DORA regulation. The expert emphasized that handling customer data involves a high degree of responsibility: "We have been trusted by our customers to keep their data," they stated. Compliance is not merely a legal requirement, but also a matter of reputation and trust. The legal provisions are made operational through technical implementations such as system access controls, data classification, and strict data deletion protocols once a customer relationship ends. (Walz M. 14 February 2025)

5.1.2 Effectiveness and Enforcement

Despite the centrality of these laws in the financial sector, the expert pointed out that enforcement mechanisms often lack consistency. While the potential for heavy penalties under GDPR (up to 4% of a company's global turnover) serves as a deterrent, actual audits or enforcement actions are rare. Most companies comply out of precaution rather than pressure. In practice, enforcement is largely reactive, taking place only after complaints or breaches have occurred. This reactive nature

raises questions about the overall efficiency and reach of current privacy frameworks. (Walz 14 February 2025)

5.1.3 Implementation Challenges

From a technical perspective, one of the most complex aspects of data protection is identifying the full scope of systems in which personal data is stored. This includes both primary operational systems and more obscure data sources like logs and backups. The expert noted that data deletion, especially across backups and redundant systems, remains a persistent technical and legal challenge. Furthermore, issues of data localization arise, particularly in relation to cloud services. The company follows strict internal policies that prevent data storage in regions deemed insecure, such as the United States or parts of Asia, highlighting a desire to maintain data sovereignty within politically and legally aligned jurisdictions. (Walz 14 February 2025)

5.1.4 Public Awareness and the “Privacy Paradox”

The expert expressed concern over the general public’s lack of awareness regarding the extent to which their data is harvested and shared. While laws exist to protect individuals, the public often doesn’t realize how extensively their behavior is tracked, especially through smartphones and social media. Many people justify their indifference with the argument that they “have nothing to hide,” which, according to the participant, ignores the deeper implications of data commodification. This contradiction between expressed concern and actual behavior, often called the “privacy paradox” (Gerber, Gerber & Volkamer 2018), was repeatedly emphasized. (Walz 14 February 2025)

5.1.5 The Importance of Digital Literacy

A major theme throughout the interview was the critical role of digital literacy. The expert described it as “the only way to go,” suggesting that long-term change in behavior and awareness must begin through education, especially at a young age. Adults, they argued, often lack the time or resources to fully grasp the implications of digital surveillance.. (Walz 14 February 2025)

5.1.6 Trust, Social Media, and Digital Sovereignty

Another pressing issue raised was the public's relationship with digital platforms, particularly those that dominate the communication ecosystem. The expert lamented that trust in these platforms is largely misplaced and that alternatives, particularly those offering strong privacy guarantees, are either inaccessible or unknown to the general public. Social media was described as a powerful force that can shape public opinion and behavior, often invisibly. The control exercised by a handful of private actors over public discourse and data infrastructures, they suggested, presents a significant threat to both individual and national sovereignty. (Walz 14 February 2025)

5.1.7 Artificial Intelligence and the Future of Regulation

Looking to the future, the expert expressed concern over the role of artificial intelligence in data governance. They raised questions around bias, transparency, and accountability, asking, "Who controls the AI? What bias does it have?" As AI systems become more deeply embedded in everyday services, the risks of centralizing power over personal data are increasing. This leads to a growing need for robust and independent governance mechanisms, as well as the development of European or Swiss alternatives to current tech monopolies. (Walz 14 February 2025)

5.1.8 Recommendations and Outlook

In closing, the expert recommended that future research and policymaking prioritize digital education and accessibility, emphasizing the need for public empowerment through knowledge. They also suggested interviewing educators to explore how digital literacy can be better integrated into curricula and emphasized the importance of legal clarity for citizens. For the broader structural challenges, they advocated for breaking monopolies and encouraging decentralized, privacy-respecting platforms as essential steps toward meaningful digital sovereignty.

This interview underscored the complex and layered reality of data protection in practice. It revealed a gap between the legal frameworks in place and the public's ability to act within them. Furthermore, it highlighted the pressing need to approach privacy not just as a regulatory issue, but as a deeply social and cultural one, where literacy, trust, and empowerment are just as critical as technical compliance.

5.2 Survey results

The survey confirmed several trends observed in the interviews. A majority of respondents were aware of the GDPR and FADP but only a minority felt confident in their understanding or application. The level of digital literacy and data protection practices correlated strongly with education level and age group, with younger respondents (digital natives) showing more comfort with privacy tools, yet not necessarily more legal awareness.

Trust levels were notably low regarding tech corporations, and moderately low for government institutions. Interestingly, a significant portion of participants supported stronger national measures to protect digital sovereignty, including local cloud infrastructure and stricter data handling standards for foreign companies.

The data also illustrated that while individuals often claim to value privacy, this is not always reflected in behavior, a phenomenon sometimes referred to as the privacy paradox. For example, only 1 of the 107 respondents answered that they always read the privacy policies. Not reading terms of services as well as privacy policies means consenting to anything. The famous Facebook/Cambridge Analytica case of 2018 highlights this perfectly (Granville March 2018)

5.3 Improvements proposal

Based on the empirical findings, the following improvements are proposed:

- **Clearer and more accessible communication of privacy laws:** Although legal frameworks like the GDPR and FADP exist to safeguard individuals' rights, the interview and survey data reveal a significant gap between these protections and public understanding. Many participants expressed uncertainty about their rights or struggled to navigate dense legal language. To address this, privacy laws need to be communicated in plain, accessible language. Public institutions could launch educational campaigns via civic platforms, social media, public transport, and digital services to raise awareness. Schools, libraries, and municipalities can play a key role in making privacy information a part of everyday civic discourse. The goal is to demystify data protection and transform it from a niche legal topic into a widely understood social right.

- **Integration of digital rights education into digital literacy curricula:** The interview with the information security officer strongly emphasized that literacy is key to sovereignty in the digital age. Survey results also showed that many individuals lacked the knowledge or confidence to act even when aware of their rights. As such, digital literacy education must include modules on privacy, data protection, and personal data management. This could be integrated into school curricula, lifelong learning programs, or vocational training. More than theory, these programs should offer practical exercises: understanding cookies, adjusting app permissions, recognizing dark patterns, and using privacy-enhancing tools (e.g., VPNs, encrypted messaging). Empowering citizens with digital rights knowledge strengthens individual agency and closes the gap between law and lived experience.
- **User-friendly tools and interfaces:** Even when people are aware of their data rights, the process of acting on them. For example, requesting access, correction, or deletion of personal data can be intimidating or overly complex. From the empirical findings, it is clear that ease of access is crucial. Companies and institutions should be encouraged or required to implement user-friendly dashboards that allow individuals to manage their data transparently. These tools should be available in multiple languages, accessible across devices, and built with inclusivity in mind (e.g., for elderly users or those with disabilities). Automated processes (e.g., one-click data deletion) and clear documentation can further lower the threshold for action.
- **Policy-level incentives for transparent platforms:** Participants in both survey and interviews expressed distrust in large tech platforms, while acknowledging their dominance. This suggests a market imbalance that favors convenience over privacy. To counter this, governments and regulatory bodies should introduce incentives (e.g. financial, infrastructural, or reputational) for services that prioritize user privacy. For example, Swiss-based cloud providers or decentralized applications that meet strict transparency and security standards could receive public funding, procurement preference, or certification marks. Such policies not only encourage the growth of ethical alternatives, but also challenge monopolies that erode both personal and national digital sovereignty.
- **Collaboration between civil society, academia, and policymakers:** A recurring theme in the interview was the need for cross-sectoral dialogue. Privacy and digital sovereignty are not challenges that can be solved by governments or companies alone. Civil society

organizations often work on the frontlines of privacy education and digital rights advocacy, while academics bring rigorous analysis and long-term thinking. Policymakers benefit from these perspectives to craft responsive and inclusive legislation. Creating collaborative frameworks, such as advisory councils, participatory governance platforms, or co-creation labs, can ensure that privacy policies are informed by real-world experience and that digital governance remains democratic and transparent.

5.4 Theoretical framework conclusions

This thesis built its analysis on five key concepts: privacy, data protection, digital literacy, trust in digital systems, and digital sovereignty. The empirical data confirms the strong interconnectedness between these concepts. Privacy and data protection are essential components of digital autonomy; however, without adequate digital literacy, these rights often remain theoretical and underused. Furthermore, trust in digital systems is increasingly undermined by the opacity of data policies and the overwhelming dominance of foreign digital service providers, highlighting the urgent need for coherent and transparent national digital strategies. The concept of digital sovereignty, while often discussed in geopolitical terms, must also be understood on a personal level. Individuals require both the knowledge and the tools to reclaim control over their digital identities (Zuboff 2019; Fratini et al. 2024). Ultimately, the findings of this thesis suggest that achieving digital sovereignty is not merely a question of state infrastructure or regulation, but a broader, collective social process grounded in education, empowerment, and critical engagement with technology.

5.5 Conclusion

This study explored how privacy laws and the broader concept of digital sovereignty are experienced by individuals in Switzerland. By combining quantitative and qualitative methods, it has shown that although regulatory frameworks exist to protect data, the social effectiveness of these laws depends on awareness, accessibility, and trust.

A clear gap exists between legal provisions and lived experience. Bridging this gap will require efforts not only from policymakers and technologists but also from educators, civil society, and

citizens themselves. In a time of growing datafication, digital rights must be reimagined not just as protections, but as instruments of empowerment and self-determination.

This thesis contributes to that re-imagination by centering the human dimension of digital sovereignty, one that is grounded in awareness, participation, and collective responsibility.

Sources

Abramova, O., Wagner, A. & Olt, C.M. June 2022. 'One for all, all for one: Social considerations in user acceptance of contact tracing apps using longitudinal evidence from Germany and Switzerland', International Journal of Information Management, 64, p. 102473. DOI: https://doi.org/10.1016/j.ijinfomgt.2022.102473. Accessed: 02 February 2025.

Advisors, S.C. 2020. 'Schrems II a summary - all you need to know', GDPR Summary, 23 November. Available at: https://www.gdprsummary.com/schrems-ii/ Accessed: 4 February 2025.

Alakrash, H.M. & Abdul Razak, N. 8 November 2021. 'Technology-Based Language Learning: Investigation of Digital Technology and Digital Literacy', Sustainability, 13(21), p. 12304. DOI: https://doi.org/10.3390/su132112304. Accessed: 27 January 2025.

Al-Saqaf, W. & Seidler, N. 11 November 2017. 'Blockchain technology for social impact: opportunities and challenges ahead', Journal of Cyber Policy, 2(3), pp. 338–354. DOI: https://doi.org/10.1080/23738871.2017.1400084. Accessed: 03 February 2025.

Andrew, J. & Baker, M. 2021. 'The General Data Protection Regulation in the Age of Surveillance Capitalism', Journal of Business Ethics, 168(3), pp. 565–578. Accessed: 02 February 2025

Andrey M., Product Owner Service Desk. Bâloise Group. Basel.

Assemblée fédérale de la Confédération suisse,. RS 235.1 - Loi fédérale sur la protection des données (LPD). 25 september 2025.

Audrin, C. & Audrin, B. 2022. 'Key factors in digital literacy in learning and education: a systematic literature review using text mining', Education and Information Technologies, 27(6), pp. 7395–7419. DOI: https://doi.org/10.1007/s10639-021-10832-5. Accessed: 28 January 2025.

Batubara, F.R., Ubacht, J. & Janssen, M. 2018. 'Challenges of blockchain technology adoption for e-government: a systematic literature review', in Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age. New York, NY, USA: Association for Computing Machinery (dg.o '18), pp. 1–9. DOI: https://doi.org/10.1145/3209281.3209317. Accessed: 05 February 2025

Bélanger, F. & Crossler, R.E. 2011. 'Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems', MIS Quarterly, 35(4), pp. 1017–1041. DOI: https://doi.org/10.2307/41409971. Accessed: 27 Janvier 2025.

Biolo, E. s.a. 'IT literacy in primary school education system: a comparative study of Finland, French-speaking Switzerland and Italy'. URN: https://urn.fi/URN:NBN:fi:amk-2024052013412. Accessed: 02 March 2025.

Botturi, L. 2019. 'Digital and media literacy in pre-service teacher education', Nordic Journal of Digital Literacy, 14(3–4), pp. 147–163. DOI: https://doi.org/10.18261/issn.1891-943x-2019-03-04-05. Accessed: 10 February 2025.

British Columbia Government. 2022. Digital Literacy - Province of British Columbia. Province of British Columbia. Available at: https://www2.gov.bc.ca/gov/content/education-training/k-12/teach/resources-for-teachers/digital-literacy Accessed: 27 January 2025.

Bühler, N., 2024. 'Between data providers and concerned citizens: Exploring participation in precision public health in Switzerland', Public Understanding of Science, 33(1), pp. 105–120. DOI: https://doi.org/10.1177/09636625231183265. Accessed: 02 February 2025.

Chander, A. & Sun, H. 2021. 'Sovereignty 2.0'. Rochester, NY: Social Science Research Network. DOI: https://doi.org/10.2139/ssrn.3904949. Accessed: 25 April 2025.

CIIP s.a. portail.ciip.ch. Available at: https://portail.ciip.ch. Accessed: 10 March 2025.

Clausius, M. 2022. 'The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes', Washington University Global Studies Law Review, 21, p. 273.

Coccoli, J. 2017. 'The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era', Peace Human Rights Governance, 1(Peace Human Rights Governance 1/2), pp. 223–250.

Couture, S. and Toupin, S. 2019. 'What does the notion of "sovereignty" mean when referring to the digital?', New Media & Society, 21(10), pp. 2305–2322. DOIt: https://doi.org/10.1177/1461444819865984. Accessed: 20 January 2025.

Custers, B. 2022. ‘New digital rights: Imagining additional fundamental rights for the digital era’, Computer Law & Security Review, 44, p. 105636. DOI: https://doi.org/10.1016/j.clsr.2021.105636. Accessed: 29 January 2025

EDK s.a. Lehrplan 21. Available at: https://v-fe.lehrplan.ch/index.php Accessed: 10 March 2025.

EDK s.a. Scolarité obligatoire. Available at: https://www.edk.ch/fr/systeme-educatif-ch/obligatoire Accessed: 10 March 2025.

European Data Protection Supervisor 2025. Data Protection Officer (DPO). URL: https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en Accessed: 25 April 2025.

de Haan s.a. ‘Digital Literacy and Safety Skills’.

Dessislava L. s.a. Droit pénal informatique. Presentation material for the Law and Ethics course on Moodle. Haute école de Gestion Genève. Accessed: 08 February 2025.

Diggelmann, O. & Cleis, M.N. 2014. ‘How the Right to Privacy Became a Human Right’, Human Rights Law Review, 14(3), pp. 441–458. URL: https://doi.org/10.1093/hrlr/ngu014. Accessed: 28 January 2025.

Duranti, L. and Rogers, C. 2012. ‘Trust in digital records: An increasingly cloudy legal area’, Computer Law & Security Review, 28(5), pp. 522–531. DOI: https://doi.org/10.1016/j.clsr.2012.07.009. Accessed: 20 January 2025.

European Union Agency for Fundamental Rights. 2013. What are fundamental rights? URL: https://fra.europa.eu/en/content/what-are-fundamental-rights. Accessed: 29 January 2025.

Falchuk, B., Loeb, S. & Neff, R. 2018. ‘The Social Metaverse: Battle for Privacy’, IEEE Technology and Society Magazine, 37(2), pp. 52–61. DOI: https://doi.org/10.1109/MTS.2018.2826060. Accessed: 20 January 2025.

Falkner, G., Heidebrecht S., Obendiek A. & Seidl T. 2024. ‘Digital sovereignty - Rhetoric and reality’, Journal of European Public Policy, 31(8), pp. 2099–2120. DOI: https://doi.org/10.1080/13501763.2024.2358984. Accessed: 25 January 2025.

Fang, W., Wen X.Z., Zhen Y. & Zhou M. 2017. 'A Survey of Big Data Security and Privacy Preserving', IETE Technical Review, 34(5), pp. 544–560. DOI: https://doi.org/10.1080/02564602.2016.1215269. Accessed: 03 February 2025.

Farias-Gaytan, S., Aguaded, I. & Ramirez-Montoya, M.-S. 2023. 'Digital transformation and digital literacy in the context of complexity within higher education institutions: a systematic literature review', Humanities and Social Sciences Communications, 10(1), pp. 1–11. DOI: https://doi.org/10.1057/s41599-023-01875-9. Accessed: 26 January 2025.

Federal Data Protection and Information Commissioner s.a. Welcome to the FDPIC. URL. https://www.edoeb.admin.ch/en. Accessed: 27 January 2025.

Finck, M. 2018. 'Blockchains and Data Protection in the European Union', European Data Protection Law Review (EDPL), 4, p. 17. Accessed: 02 February 2025.

Flonk, D., Jachtenfuchs, M. & Obendiek, A. 2024. 'Controlling internet content in the EU: towards digital sovereignty', Journal of European Public Policy, 31(8), pp. 2316–2342. DOI: https://doi.org/10.1080/13501763.2024.2309179. Accessed: 26 January 2025.

Floridi, L. 2005. 'The Ontological Interpretation of Informational Privacy', Ethics and Information Technology, 7(4), pp. 185–200. DOI: https://doi.org/10.1007/s10676-006-0001-7. Accessed: 29 January 2025.

Floridi, L. 2016. 'On Human Dignity as a Foundation for the Right to Privacy', Philosophy & Technology, 29(4), pp. 307–312. DOI: https://doi.org/10.1007/s13347-016-0220-8. Accessed: 28 January 2025.

Floridi, L. 2021. 'The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU'. Rochester, NY: Social Science Research Network. DOI: https://doi.org/10.2139/ssrn.3827089. Accessed: 25 April 2025.

Fratini, S., Hine E., Novelli C., Roberts H. & Floridi L. 2024. 'Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models', Digital Society, 3(3), p. 59. DOI: https://doi.org/10.1007/s44206-024-00146-7. Accessed: 28 January 2025.

Fratini, S. 2024. ‘Performing Privacy Culture. The Platform Threema and the Contestation of Surveillance Made in Switzerland’, Studi culturali [Preprint], (1/2024). DOI: https://doi.org/10.1405/113065. Accessed: 02 February 2025.

Fratini, S. & Musiani, F. 2024. ‘Data localization as contested and narrated security in the age of digital sovereignty: the case of Switzerland’, Information, Communication & Society, pp. 1–19. DOI: https://doi.org/10.1080/1369118X.2024.2362302. Accessed: 23 January 2025.

Fuster, G.G. 2014. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Springer Science & Business.

GDPR Summary. 2021. ‘Data Protection Officer (DPO) guide’. URL: https://www.gdprsummary.com/data-protection-officer/. Accessed: 27 January 2025.

Gellert, R. & Gutwirth, S. 2013. ‘The legal construction of privacy and data protection’, Computer Law & Security Review, 29(5), pp. 522–530. DOI: https://doi.org/10.1016/j.clsr.2013.07.005. Accessed: 02 February 2025.

Gerber, N., Gerber, P. & Volkamer, M. 2018. ‘Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior’, Computers & Security, 77, pp. 226–261. DOI: https://doi.org/10.1016/j.cose.2018.04.002. Accessed: 27 April 2025.

Goldberg, I. 2003. ‘Privacy-Enhancing Technologies for the Internet, II: Five Years Later’, in R. Dingledine and P. Syverson (eds) Privacy Enhancing Technologies. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), pp. 1–12. DOI: https://doi.org/10.1007/3-540-36467-6_1. Accessed: 03 February 2025.

Goodin, D. 2023. Leak of MSI UEFI signing keys stokes fears of “doomsday” supply chain attack, Ars Technica. URL: https://arstechnica.com/information-technology/2023/05/leak-of-msi-uefi-signing-keys-stokes-concerns-of-doomsday-supply-chain-attack/ Accessed: 3 February 2025.

Graeber, M. s.a. ‘Subverting Trust in Windows’. URL: https://specterops.io/wp-content/uploads/sites/3/2022/06/SpecterOps_Subverting_Trust_in_Windows.pdf. Accessed: 25 January 2025

Granville, K. 2018. ‘Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens’, The New York Times, 19 March. URL: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html Accessed: 23 April 2025.

Grottola, S.P. 2022. ‘Responsible behaviour in cyberspace: engaging the private sector through tech diplomacy’, Rivista di Digital Politics [Preprint], (3/2022). Available at: https://doi.org/10.53227/106454. Accessed: 02 February 2025.

Hildebrandt, M. & Tielemans, L. 2013. ‘Data protection by design and technology neutral law’, Computer Law & Security Review, 29(5), pp. 509–521. DOI: https://doi.org/10.1016/j.clsr.2013.07.004. Accessed: 02 February 2025.

Hobbs, R. & Moore D.C. s.a. ‘POWERFUL VOICES FOR KIDS: DIGITAL AND MEDIA LITERACY IN ELEMENTARY SCHOOL’.

Hofmann, D. 2024 ‘FemTech: empowering reproductive rights or FEM-TRAP for surveillance?’, Medical Law Review, 32(4), pp. 468–485. DOI: https://doi.org/10.1093/medlaw/fwae035. Accessed: 05 February 2025.

Husfeldt, V. & Alt, S. 2021. ‘From Information Literacy to Data Literacy Education: A Case Study from Switzerland’, in. Glückstadt: Werner Hülsbusch, pp. 73–77. DOI: https://doi.org/10.5283/epub.44938. Accessed: 30 January 2025.

Jain, P., Gyanchandani, M. & Khare, N. 2016 ‘Big data privacy: a technological perspective and review’, Journal of Big Data, 3(1), p. 25. DOI: https://doi.org/10.1186/s40537-016-0059-y. Accessed: 29 January 2025.

Kafi, M.A. & Akter, N. 2023. ‘Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection’, American Journal of Trade and Policy, 10(1), pp. 15–26. DOI: https://doi.org/10.18034/ajtp.v10i1.659. Accessed 02 February 2025.

Klauser, F. 2004. ‘A Comparison of the Impact of Protective and Preservative Video Surveillance on Urban Territoriality: the case of Switzerland’, Surveillance & Society, 2(2/3). DOI: https://doi.org/10.24908/ss.v2i2/3.3371. Accessed: 01 February 2025.

Kuner, C. 2017. ‘Reality and Illusion in EU Data Transfer Regulation Post Schrems’, German Law Journal, 18(4), pp. 881–918. DOI: https://doi.org/10.1017/S2071832200022197. Accessed: 26 January 2025.

Kuner, C., Svantesson D.J.B., Cate F.H., Lynskey O., Millard C. 2017. ‘The rise of cybersecurity and its impact on data protection’, International Data Privacy Law, 7(2), pp. 73–75. DOI: https://doi.org/10.1093/idpl/ipx009. Accessed: 01 February 2025

Livingstone, S. 2014. ‘Developing social media literacy: How children learn to interpret risky opportunities on social network sites’, Communications, 39(3). DOI: https://doi.org/10.1515/commun-2014-0113. Accessed: 28 January 2025.

Lorenzet, A. 2015. ‘The «media scenes» of datification. The technoscientific controversy on privacy in Italian newspapers’, Rassegna Italiana di Sociologia [Preprint], (3-4/2015). DOI: https://doi.org/10.1423/81806. Accessed: 02 February 2025.

Lucchi, N. 2024. ‘ChatGPT: A Case Study on Copyright Challenges for Generative Artificial Intelligence Systems’, European Journal of Risk Regulation, 15(3), pp. 602–624. DOI: https://doi.org/10.1017/err.2023.59. Accessed: 03 February 2025.

Margulis, S.T. 2003. ‘Privacy as a Social Issue and Behavioral Concept’, Journal of Social Issues, 59(2), pp. 243–261. DOI: https://doi.org/10.1111/1540-4560.00063. Accessed: 20 January 2025.

Martani, A., Egli P., Widmer M. & Elger B. 2020. ‘Data protection and biomedical research in Switzerland: setting the record straight’, Swiss Medical Weekly, 150(3536), pp. w20332–w20332. DOI: https://doi.org/10.4414/smw.2020.20332. Accessed: 14 January 2025.

Martani, A. Geneviève L.D., Wangmo T., Maurer J., Crameri K., Erard F., Spoendlin J., Pauli-Magnus C., Pittet V., Sengstag T., Soldini E., Hirschel B., Borisch B., Weber C.K., Zwahlen M. & Elger B.S. 2023. ‘Sensing the (digital) pulse. Future steps for improving the secondary use of data for research in Switzerland’, DIGITAL HEALTH, 9, p. 20552076231169826. DOI: https://doi.org/10.1177/20552076231169826. Accessed: 24 January 2025.

Martin, A. & Grudziecki, J. 2006. ‘DigEuLit: Concepts and Tools for Digital Literacy Development’, Innovation in Teaching and Learning in Information and Computer Sciences, 5(4), pp. 249–267. DOI: https://doi.org/10.11120/ital.2006.05040249. Accessed: 10 March 2025

Martin, K.D. & Murphy, P.E. 2017. ‘The role of data privacy in marketing’, Journal of the Academy of Marketing Science, 45(2), pp. 135–155. DOI: https://doi.org/10.1007/s11747-016-0495-4. Accessed: 26 January 2025.

Mathioudaki, K. & Gkaravelas, K. 2023. ‘Critical literacy through Information and Communication Technologies in the primary educational systems of Spain and Switzerland: A comparative study based on the example of WebQuests’, International Journal of Educational Innovation and Research, 2(1), pp. 47–58. DOI: https://doi.org/10.31949/ijeir.v2i1.3461. Accessed: 29 January 2025.

Mehrnezhad, M., Van Der Merwe, T. & Catt, M. 2024. ‘Mind the FemTech gap: regulation failings and exploitative systems’, Frontiers in the Internet of Things, 3. DOI: https://doi.org/10.3389/friot.2024.1296599. Accessed: 02 February 2025.

Milanovic, M. 2015. ‘Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age’, Harvard International Law Journal, 56, p. 81. Accessed: 28 January 2025.

Milenkova, V. & Lendzhova, V. 2021. ‘Digital Citizenship and Digital Literacy in the Conditions of Social Crisis’, Computers, 10(4), p. 40. DOI: https://doi.org/10.3390/computers10040040.

Mueller, M.L. 2020. ‘Against Sovereignty in Cyberspace’, International Studies Review, 22(4), pp. 779–801. DOI: https://doi.org/10.1093/isr/viz044. Accessed: 27 January 2025.

Murray, N. 2020. ‘Review: Permanent Record by Edward Snowden The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power by Shoshana Zuboff’, Race & Class, 61(4), pp. 96–102. DOI: https://doi.org/10.1177/0306396820908752. Accessed: 27 January 2025.

Nissim, K. & Wood, A. 2018. ‘Is privacy privacy?’, Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 376(2128), p. 20170358. DOI: https://doi.org/10.1098/rsta.2017.0358. Accessed: 27 January 2025.

Nyst, C. & Falchetta, T. 2017. ‘The Right to Privacy in the Digital Age’, Journal of Human Rights Practice, 9(1), pp. 104–118. DOI: https://doi.org/10.1093/jhuman/huw026. Accessed: 04 February 2025.

Obar, J.A. & Oeldorf-Hirsch, A. 2020. ‘The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services’, Information, Communication & Society, 23(1), pp. 128–147. DOI: https://doi.org/10.1080/1369118X.2018.1486870. Accessed: 03 February 2025

Office fédéral de la justice s.a. Renforcement de la protection des données. URL: https://www.bj.admin.ch/bj/fr/home/staat/gesetzgebung/archiv/datenschutzstaerkung.html Accessed: 25 April 2025.

Oh, S.S., Kim K.-A., Kim M. Oh J., Chu S.H. & Choi J. 2021. ‘Measurement of Digital Literacy Among Older Adults: Systematic Review’, Journal of Medical Internet Research, 23(2), p. e26145. DOI: https://doi.org/10.2196/26145. Accessed: 27 January 2025.

Olsen, T. & Mahler, T. 2007. ‘Identity management and data protection law: Risk, responsibility and compliance in “Circles of Trust” – Part II’, Computer Law & Security Review, 23(5), pp. 415–426. DOI: https://doi.org/10.1016/j.clsr.2007.07.001. Accessed: 28 January 2025.

paolomatarazzo 2024. Windows 11 security book - Virus and threat protection. URL: https://learn.microsoft.com/en-us/windows/security/book/operating-system-security-virus-and-threat-protection. Accessed: 27 January 2025.

Philpott, D. 1995. ‘Sovereignty: An Introduction and Brief History’, Journal of International Affairs, 48(2), pp. 353–368.

Piano di Studio della scuolla dell’obbligo s.a. Portale del Piano di studio. URL: https://pianodistudio.edu.ti.ch/. Accessed: 10 March 2025.

Pletscher, F., Mändli Lerch, K. & Glinz, D. 2022. ‘Willingness to share anonymised routinely collected clinical health data in Switzerland: a cross-sectional survey’, Swiss Medical Weekly, 152(2324), pp. w30182–w30182. DOI: https://doi.org/10.4414/SMW.2022.w30182. Accessed: 02 February 2025.

Purtova, N. 2018. ‘The law of everything. Broad concept of personal data and future of EU data protection law’, Law, Innovation and Technology, 10(1), pp. 40–81. DOI: https://doi.org/10.1080/17579961.2018.1452176. Accessed: 02 February 2025.

Radovanović, D. 2023. Digital Literacy and Inclusion: Stories, Platforms, Communities. Cham, SWITZERLAND: Springer International Publishing AG. URL: http://ebookcentral.proquest.com/lib/haaga/detail.action?docID=30765488. Accessed: 27 January 2025.

Rawat, D.B., Doku, R. & Garuba, M. 2021. ‘Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security’, IEEE Transactions on Services Computing, 14(6), pp. 2055–2072. DOI: https://doi.org/10.1109/TSC.2019.2907247. Accessed: 02 February 2025.

Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Regulation (EU) 2016/679 of the european parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC General Data Protection Regulation), 27 April 2016.

Reijers, W., O’Brolcháin, F. & Haynes, P. 2016. ‘Governance in Blockchain Technologies & Social Contract Theories’, Ledger, 1, pp. 134–151. DOI: https://doi.org/10.5195/ledger.2016.62. Accessed: 03 February 2025.

Ruan, Y. & Durresi, A. 2016. ‘A survey of trust management systems for online social communities – Trust modeling, trust inference and attacks’, Knowledge-Based Systems, 106, pp. 150–163. DOI: https://doi.org/10.1016/j.knosys.2016.05.042. Accessed: 27 January 2025.

Rubinstein, I.S. & Good, N. 2013. ‘Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents’, Berkeley Technology Law Journal, 28(2), pp. 1333–1413. Accessed: 27 January 2025.

Salehzadeh Niksirat, K., Korka D., Jacquemin Q., Vanini C., Humbert M., Cherubini M., Métille S. & Huguenin K. 2024. ‘Security and Privacy with Second-Hand Storage Devices: A User-Centric

Perspective from Switzerland', Proceedings on Privacy Enhancing Technologies, 2024(2), pp. 412–433. DOI: https://doi.org/10.56553/popets-2024-0057. Accessed: 02 February 2025.

Sartor, G., Stølen K., Winsborough W.H., Martinelli F. & Massacci F. 2006. 'Privacy, Reputation, and Trust: Some Implications for Data Protection', in K. Stølen et al. (eds) Trust Management. Berlin, Heidelberg: Springer, pp. 354–366. DOI: https://doi.org/10.1007/11755593_26. Accessed: 27 January 2025.

Schachtner, C. & Baumann, N. 2025. 'Digital competencies for municipalities – Findings from Switzerland as a role model for smart regions within the European Union member states', Smart Cities and Regional Development (SCRD) Journal, 9(1), pp. 99–106. DOI: https://doi.org/10.25019/zbe76975. Accessed: 27 January 2025.

Sheikh, H. 2022. 'European Digital Sovereignty: A Layered Approach', Digital Society, 1(3), p. 25. DOI: https://doi.org/10.1007/s44206-022-00025-z. Accessed: 25 April 2025.

Ocelik, V., Kolk, A. & Irion, K. 2025 'Shifting Battlegrounds: Corporate Political Activity in the EU General Data Protection Regulation. DOI: https://doi.org/10.1177/00076503241306958. Accessed: 02 February 2025.

S.M.E. s.a. Data protection. Available at: https://www.kmu.admin.ch/kmu/en/home/fakten-und-trends/digitalisierung/datenschutz.html. Accessed: 25 April 2025.

Smith, M., Szongott, C., Henne B. & von Voigt, G. 2012. 'Big data privacy issues in public social media', in 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST). 2012 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), pp. 1–6. DOI: https://doi.org/10.1109/DEST.2012.6227909. Accessed: 25 January 2025.

Sonnenberg, P. & Hoffmann, T. 2022. 'Data Protection Revisited - Report on the Law of Data Disclosure in Switzerland'. Rochester, NY: Social Science Research Network. URL: https://papers.ssrn.com/abstract=4458157 Accessed: 27 January 2025.

Stadelmann-Steffen, I. & Rihm, M. 2022 'Switzerland: Political Developments and Data in 2021', European Journal of Political Research Political Data Yearbook, 61(1), pp. 450–468. DOI: https://doi.org/10.1111/2047-8852.12361. Accessed: 26 January 2025.

Sule, M.-J., Zennaro, M. & Thomas, G. (2021) 'Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends', Technology in Society, 67, p. 101734. DOI: https://doi.org/10.1016/j.techsoc.2021.101734. Accessed: 02 February 2025.

Sun, Y., Zhang, J., Xiong, Y. & Zhu, G. 2014. 'Data Security and Privacy in Cloud Computing', International Journal of Distributed Sensor Networks, 10(7), p. 190903. DOI: https://doi.org/10.1155/2014/190903. Accessed: 03 February 2025.

Swiss federal authorities s.a. Basic knowledge. URL: https://www.edoeb.admin.ch/en/basic-knowledge/ Accessed: 25 April 2025.

Ting, H.L.J., Kang, X., Li T., Wang, H. & Chu, C.-K. 2021. 'On the Trust and Trust Modeling for the Future Fully-Connected Digital World: A Comprehensive Study', IEEE Access, 9, pp. 106743–106783. DOI: https://doi.org/10.1109/ACCESS.2021.3100767. Accessed: 27 January 2025.

Tinmaz, H., Lee, Y.-T., Fanea-Ivanovici, M. & Baber, H. 2022. 'A systematic review on digital literacy', Smart Learning Environments, 9(1), p. 21. DOI: https://doi.org/10.1186/s40561-022-00204-y. Accessed: 27 January 2025.

Tracol, X. 2020. '"Schrems II": The return of the Privacy Shield', Computer Law & Security Review, 39, p. 105484. DOI: https://doi.org/10.1016/j.clsr.2020.105484. Accessed: 23 January 2025.

Unesco. 2018. A Global framework of reference on digital literacy skills for indicators 4.4.2; UIS information paper; Vol.:51; - 265403eng.pdf (s.a.). Available at: https://unesdoc.unesco.org/in/documentViewer.xhtml?v=2.1.196&id=p::usmarcdef_0000265403&file=/in/rest/annotationSVC/DownloadWatermarkedAttachment/attach_import_05582007-8091-4d65-bb0e-a459fa55483b%3F_%3D265403eng.pdf&locale=en&multi=true&ark=/ark:/48223/pf0000265403/PDF/265403eng.pdf#%5B%7B%22num%22%3A10%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C54%2C681%2C0%5D Accessed: 27 January 2025.

United Nations. 1948. Universal Declaration of Human Rights, United Nations. URL: https://www.un.org/en/about-us/universal-declaration-of-human-rights Accessed: 29 January 2025.

U.S. government 2023. An introduction to digital governance. URL: https://digital.gov/resources/an-introduction-to-digital-governance/. Accessed 27 January 2025.

Van Den Hoven, J. 2008. 'Information Technology, Privacy, and the Protection of Personal Data', in J. van den Hoven and J. Weckert (eds) Information Technology and Moral Philosophy. Cambridge: Cambridge University Press (Cambridge Studies in Philosophy and Public Policy), pp. 301–321. DOI: https://doi.org/10.1017/CBO9780511498725.016. Accessed: 01 February 2025.

Walz M., Senior IT Security Governance Specialist. Bâloise. Interview. Basel.

Warren, S.D. & Brandeis, L.D. 1890. 'The Right to Privacy', Harvard Law Review, 4(5), pp. 193–220. DOI: https://doi.org/10.2307/1321160. Accessed: 22 January 2025.

Wedlake, S. & Bugre, C. 2023. 'The Potential of Digital Literacy to Curb Problematic Information: An Integrative Literature Review', in I. Sserwanga et al. (eds) Information for a Better World: Normality, Virtuality, Physicality, Inclusivity. Cham: Springer Nature Switzerland, pp. 395–404. DOI: https://doi.org/10.1007/978-3-031-28035-1_28. Accessed: 01 February 2025.

Westin, A.F. 2003. 'Social and Political Dimensions of Privacy', Journal of Social Issues, 59(2), pp. 431–453. DOI: https://doi.org/10.1111/1540-4560.00072. Accessed: 27 January 2025.

Westin, A.F. 1968. 'Privacy And Freedom'. 5 Wash. & Lee L. Rev. 166. URL: https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20. Accessed: 25 January 2025.

Wolff, R.P. 1998. In Defense of Anarchism. 1st edn. University of California Press. DOI: https://doi.org/10.2307/jj.8501193. Accessed: 10 March 2025

Wylde V., Rawindaran N., Lawrence J., Balasubramanian R., Prakash E., Jayal A., Khan I., Hewage C. & Platts J. 2022. 'Cybersecurity, Data Privacy and Blockchain: A Review', SN Computer Science, 3(2), p. 127. DOI: https://doi.org/10.1007/s42979-022-01020-4. Accessed: 02 February 2025.

Yu, S. 2016. 'Big Privacy: Challenges and Opportunities of Privacy Study in the Age of Big Data', IEEE Access, 4, pp. 2751–2763. DOI: https://doi.org/10.1109/ACCESS.2016.2577036. Accessed: 27 January 2025.

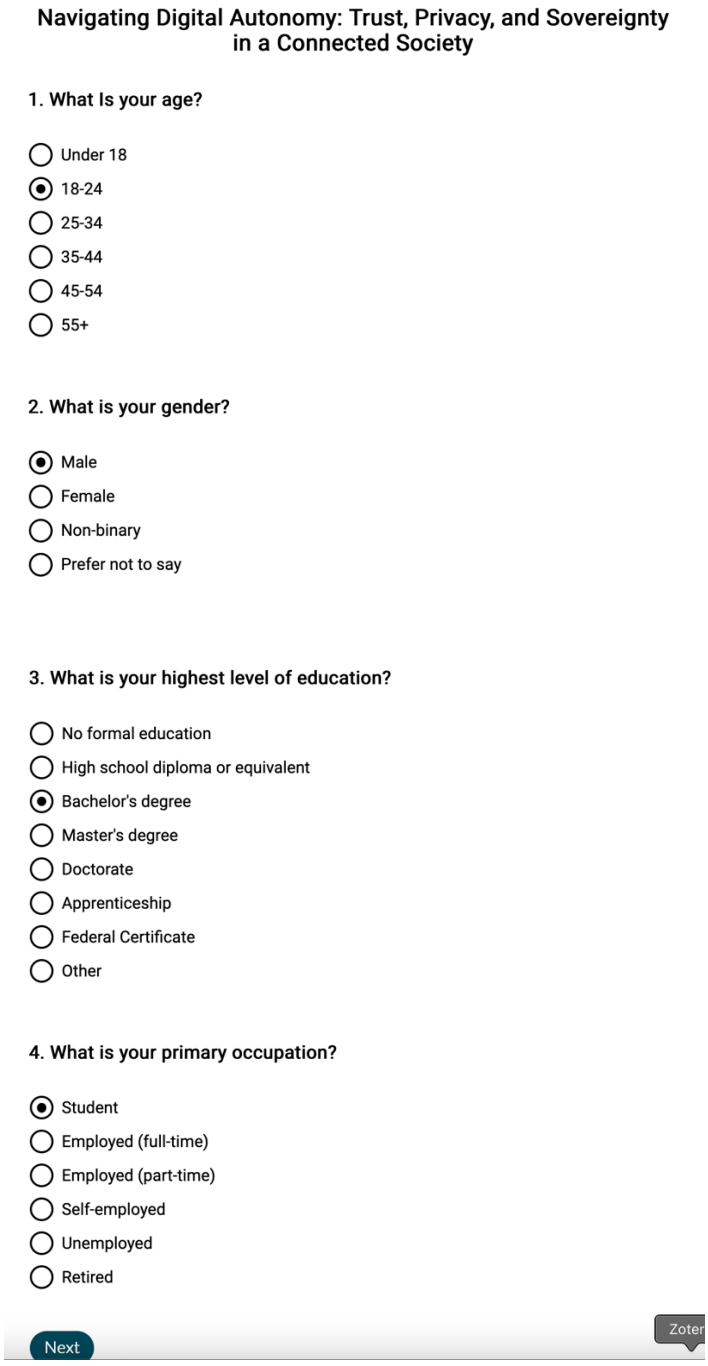
Zeffiro, A., Niessen, G., Oberst, C., McEwan, S., Cochrane, A.-C, & Durand, J. 2022. ‘Discourses on cybersecurity. The politics of the data breach as a security crisis’, Rivista di Digital Politics [Preprint], (3/2022). DOI: https://doi.org/10.53227/106451. Accessed: 02 February 2025.

Zhang, J., Hassandoust, F. & Williams, J. 2020. ‘Online Customer Trust in the Context of the General Data Protection Regulation (GDPR)’, Pacific Asia Journal of the Association for Information Systems, 12(1). DOI: https://doi.org/10.17705/1pais.12104. Accessed: 28 January 2025.

Zuboff, S. (2019) The age of surveillance capitalism: the fight for a human future at the new frontier of power. London: Profile books.

Appendices

Appendix 1. Survey



Navigating Digital Autonomy: Trust, Privacy, and Sovereignty in a Connected Society

1. What Is your age?

- ○ Under 18
- ◉ 18-24
- ○ 25-34
- ○ 35-44
- ○ 45-54
- ○ 55+

2. What is your gender?

- ◉ Male
- ○ Female
- ○ Non-binary
- ○ Prefer not to say

3. What is your highest level of education?

- ○ No formal education
- ○ High school diploma or equivalent
- ◉ Bachelor's degree
- ○ Master's degree
- ○ Doctorate
- ○ Apprenticeship
- ○ Federal Certificate
- ○ Other

4. What is your primary occupation?

- ◉ Student
- ○ Employed (full-time)
- ○ Employed (part-time)
- ○ Self-employed
- ○ Unemployed
- ○ Retired

Next

Zoter

5. Are you familiar with the Federal Act on Data Protection (FADP) and the General Regulation on Data Protection (GDPR)

6. Do you ever read privacy policies before using an online service?

- (●) Always
- ( ) Sometimes
- ( ) Rarely
- ( ) Never

7. How well do you understand your digital rights under privacy laws?

Previous Next

8. Have you ever changed your online behavior due to privacy concerns?

- ( ) Yes
- ( ) No
- ( ) I tried but wasn't able to

9. Which of the following privacy-enhancing tools do you use regularly? (Select all that apply)

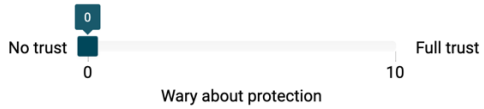
- [ ] Encrypted messaging apps (e.g., Signal, Telegram, Threema)
- [ ] VPN (Virtual Private Network)
- [ ] Browser extensions blocking trackers (e.g., uBlock, AdBlock)
- [ ] Anonymous browsing (e.g., Tor)
- [ ] None of these
- [ ] Others

10. How much control do you feel you have over your personal data online?

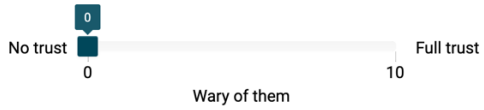
- ◯ Full control
- ◯ Some control
- ◯ Very little control
- ◯ No control

Previous Next

11. Do you trust the government to protect your digital privacy?



12. Do you trust large technology companies (Google, Meta, Amazon, etc.) to handle your personal data responsibly?



13. Do you think Switzerland should take stronger measures to protect digital sovereignty (e.g., developing national cloud services, reducing dependence on foreign tech companies)?

14. In your opinion, does the Swiss government guarantee the protection of your private data?

15. What would encourage you to take more control over your digital privacy? (Select all that apply)

- ☐ Better public awareness campaigns
- ☐ More user-friendly privacy tools
- ☐ Stronger legal protections
- ☐ Financial incentives for privacy-friendly services
- ☐ Nothing, I don't see privacy as a major issue
- ☐ Other

Appendix 2. Interview questions

Introduction

1. Can you share a brief overview of your professional background and your experience with data protection, privacy and their legislation (e.g., FADP, GDPR)?
2. Given your experience with [specific industry or sector], how have privacy laws impacted your work and the industry as a whole?
3. In your opinion, what is the primary role of privacy laws in today's digital landscape?
4. Understanding and Implementation
5. How do you assess the effectiveness of laws such as FADP or GDPR in protecting individuals' data, privacy and fostering trust in the digital ecosystem?
6. What do you see as the most significant challenges in implementing and enforcing these laws, both from a technical and a societal perspective?
7. In your experience, how well do organizations comply with FADP/GDPR regulations? What factors contribute to non-compliance, and what are the consequences of these failures?

Public Awareness and Education

1. From your perspective, how well-informed is the general public about their rights under privacy laws? Do you feel people are generally aware of the data they are sharing and how it is being used?

2. What are the most common misconceptions people have about privacy regulations, and how do these misconceptions impact their online behavior?
3. In your opinion, what are the barriers preventing people from understanding or engaging with these laws? Are these barriers primarily educational, technological, or socio-economic in nature?

Social and Technological Impacts

1. If people are aware of those laws, and considering their level of understanding, how do they influence societal trust in digital technologies and institutions (eg. Doing your taxes online, web shopping, social media etc.)
2. And in general, do you think people are concerned with their privacy at work and/or in their daily lives? How do these concerns manifest, and what impact do they have on your personal and professional life?
3. Have you observed any significant behavior changes in individuals or organizations due to privacy regulations (and your work as DPO)? How have these changes impacted the way you interact with technology and the digital world?
4. What are the implications of privacy laws on technological innovation? Do they encourage ethical and responsible development or do they hinder technological progress?
5. Improvement and Future Directions
6. What steps could be taken to make privacy laws more accessible and understandable to the public? How can we empower individuals to make informed choices about their data?
7. How can governments or organizations improve the implementation and communication of these laws?
8. Are there emerging trends or technologies that you believe will shape the future of privacy legislation? How can we ensure that these laws remain relevant and effective in a rapidly evolving technological landscape?

Conclusion

1. What are the most pressing privacy challenges facing society today, and how can we address them? What are your hopes and concerns for the future of data protection in the digital age?

2. Do you have recommendations for additional resources or individuals who could provide valuable insights for this study, such as academics, researchers, or industry leaders working in the field of privacy and data protection?