

# The Threat of Surveillance and the Need for Privacy Protections



**Martina Lindorfer**

**Abstract** In recent years, and since the introduction of the General Data Protection Regulation (GDPR) in particular, we have seen an increased interest (and concern) about the amount of private information that is collected by the applications and services we use in our daily lives. The widespread collection and commodification of personal data has been mainly driven by companies collecting, mining, and selling user profiles for targeted advertisement, a practice also referred to as “surveillance capitalism.” However, as we detail in this chapter, this is not the only form of surveillance and can be necessary and even beneficial by increasing the safety of citizens—if it is aligned with the principles of digital humanisms in providing transparency, oversight, and accountability. We also detail mechanisms users can deploy to protect their own privacy, as well as mechanisms that help to develop more privacy-friendly technologies.

## 1 Introduction

I don't know why people are so keen to put the details of their private life in public; they forget that invisibility is a superpower. (Banksy, allegedly)

We happily share intimate details of our private lives to connect with others on social networks and for the convenience of performing daily chores online and via our smartphone. This data has been coined “new oil” due to it being exploited by tech companies for their own monetary gains, i.e., “surveillance capitalism” (Zuboff, 2019). Besides the ubiquitous surveillance by Big Tech, in Western society, surveillance is mostly only associated with something that happens in less democratic countries to monitor and control citizens. This belief was upset by the revelations of Edward Snowden in 2013, when he exposed how the US National Security Agency (NSA) was collecting vast amounts of communication data, including emails and

---

M. Lindorfer (✉)

Faculty of Informatics, Research Unit Security & Privacy, Institute of Logic and Computation,  
TU Wien, Wien, Austria

e-mail: [martina.lindorfer@tuwien.ac.at](mailto:martina.lindorfer@tuwien.ac.at)

chat logs, on individuals and organizations worldwide (Gellman & Lindeman, 2013; Gellman & Poitras, 2013; Greenwald & MacAskill, 2013). While on paper being designed to collect data on American citizens and individuals in other countries, it was carried out without required warrants and put innocent individuals in the crosshairs of mass surveillance. One reason why the NSA—as well as other government agencies like the UK's Government Communications Headquarters (GCHQ)—could collect mass amounts of data at a large scale was the fact that they directly tapped Big Tech, including Google, Facebook, Microsoft, and Apple. The link between the government and the private sector has further been confirmed by reports of federal agencies in the USA, including the Department of Homeland Security and the Internal Revenue Service, buying commercially available data from data brokers (Whittaker, 2023). In countries that are notorious for surveilling their population, such as China, the entanglement of their government with private companies has long been cause for concern, resulting in the discourse about and actual banning of applications such as TikTok. Whether the concerns are warranted is up for debate, but at least for another Chinese social media platform, WeChat, research has shown that content shared by international users is being used to feed and train censorship mechanisms in China (Knockel et al., 2020). What is clear though in any jurisdiction is that any user data collected by companies is at risk of being requested by governments and law enforcement.

Tapping these tech companies for user data potentially gives governments and law enforcement information that they would not be able to collect legally (Hoofnagle, 2003), for example, through “predictive policing.” From a pragmatic point of view, it is attractive though as tech companies’ access to private user data is extensive. Technology has become an integral part of every aspect of our daily lives, and we use it through a plethora of applications (apps), for everything from emails and social networking to shopping and banking. To maximize the user experience, apps and websites collect and process an increasing amount of private information. With the rising popularity of Internet of Things (IoT) devices, we give up even more private information about our daily lives and habits for the sake of the convenience of a smart home. This does not only include seemingly harmless devices, such as smart toasters and lightbulbs, but also medical devices and fitness trackers, as well as seemingly analog devices: truly targeted TV advertisements based on viewer demographics so far have been wishful thinking (Perlberg, 2014), but new content transmission protocols, e.g., the Hybrid Broadcast Broadband TV (HbbTV) standard deployed across Europe, enable the real-time monitoring of users’ viewing preferences and integration with profiles from other sources. In other words, HbbTV turns TVs into an Internet-connected device, complete with all the customization benefits of targeted content (“addressable TV”) as well as privacy harms known from the mobile app and web domain (Tagliaro et al., 2023).

Companies use the data they collect through mobile apps, users’ browsing behavior, social media content, and data collected from smart devices, to build detailed user profiles. This private information, and user behaviors derived from it, has become a commodity: tech monopolies and shadow brokers collect and aggregate data to not only provide tailored content but also for market research and

targeted advertising (Razaghpanah et al., 2018). This process is far from transparent and includes obscure tracking methods and “various techniques [...] to prevent consumers from making a choice on privacy” (Hoofnagle et al., 2012). Furthermore, the data is not always in trustworthy and secure hands: if left unprotected from unauthorized access, social security numbers, addresses, financial records, and other highly sensitive data from billions of users are regularly leaked through data brokers and can potentially be exploited by criminals (Sherman, 2022). Most importantly, behavioral targeting is not only used to sell people products but for far more nefarious purposes: to influence public and political opinions by selectively targeting user groups with disinformation. One prominent case in this regard was Cambridge Analytica selling data harvested from Facebook to political campaigns (Rosenberg et al., 2018).

As a result, private data collection faces increased scrutiny by both legislators and users. The privacy debate has resulted in the introduction of the General Data Protection Regulation (GDPR) (European Commission, 2016) in the European Union in May 2018 and similar efforts in other countries that regulate the collection and processing of private information (see Sect. 3). Privacy is a fundamental human right that through GDPR and various other international laws and regulations around the world is being protected to varying degrees. The goal is to give individuals the ability (back) to control their personal information and keep it private. This can include information such as one’s identity, location, health conditions, social network, and personal preferences.

Still, privacy (and the individual perception of and need for privacy) is a complex topic and involves answering questions around (1) which type of data should be protected, (2) how sensitive this data is, (e.g., health information is typically seen more critically and afforded a special category of data by the GDPR than let’s say a user’s physical location or phone number), and (3) who data should be protected from. Furthermore, while everyone has the right to privacy and should be able to take steps to protect their personal information and online activities, several vulnerable groups are at higher risk of surveillance and privacy violations, ranging from threats from the government to their immediate personal surroundings:

- **Political activists:** Individuals who are involved in political activism or advocacy may be targeted for surveillance by governments or other organizations. This can include monitoring of online activity, phone calls, and physical surveillance.
- **Journalists and whistleblowers:** Journalists and whistleblowers who expose corruption or wrongdoing may also be at risk of surveillance or retaliation. This can include monitoring of communication channels, hacking of devices or accounts, and other methods of surveillance.
- **LGBTQ+ individuals:** LGBTQ+ individuals may not only face discrimination and harassment, but in certain countries even imprisonment or death, and thus may need to protect their privacy to avoid persecution.
- **Racial, ethnic, and religious minorities:** Depending on the dominant group in a country, and other factors, such as the division of state and church, minority groups might face discrimination and harassment as well.

- **People with (mental) health conditions:** Certain health conditions might also face stigmatization or discrimination, for example, in the workplace. This can reach from employees being disadvantaged based on their health to more general attacks on fundamental personal rights. In the latter case, recent regulation attempts on female reproduction pose the question on how much data is collected and shared about potential pregnancies (and their termination) that could result in legal persecution.
- **Domestic abuse and stalking survivors:** Survivors of domestic abuse or stalking (also referred to as intimate partner violence) may need to take extra precautions to protect themselves and their (online) activities from their abusers.
- **Children and young adults:** Children and young adults may be more vulnerable to online predators or cyberbullying. Privacy regulation also particularly protects individuals below a certain age as they are not mature enough to provide informed consent to data collection.

Surveillance and privacy are typically seen as opposing forces; however, in an ideal world, they should co-exist. While perceived negatively, surveillance in itself is neither inherently good nor bad and can be necessary for the greater societal good as well as national security, e.g., by providing law enforcement the means to investigate crime and ensure public safety. For example, extensive surveillance camera footage was instrumental in finding the responsible parties behind the Boston Marathon bombing in 2013 and the US Capitol Attacks in 2021. More generally, surveillance can provide:

- **Security/Safety:** Monitor and prevent criminal activity, terrorism, and other threats to public safety. For example, security cameras in public spaces can help deter crime and assist law enforcement in identifying and apprehending suspects.
- **Health:** Monitor and control the spread of infectious diseases, such as by tracking outbreaks and monitoring vaccination rates. In the case of a public health emergency, such as a pandemic, surveillance can be critical in identifying and containing the spread of the disease.
- **Traffic management:** Monitor traffic flow and congestion, which can help identify areas where infrastructure improvements are needed and can aid in emergency response planning.

Given the overall promise of using surveillance and data collection to increase safety and optimize processes, it is not surprising that also nongovernmental organizations are interested in reaping the benefits. Under the term “workplace surveillance,” companies are aiming to optimize how they hire, promote, and fire employees (Peck, 2013; Kantor & Sundaram, 2022). This includes, potentially covertly, monitoring employee activity and productivity to ensure that they are meeting their responsibilities and identify areas where performance can be improved. Whether this is legal, in particular in the context of employment laws, and how these laws still need to catch up with technology changes in the workplace (Calacci & Stein, 2023), is an open question—in addition to questions of the ethical

aspects and most importantly the efficiency of these practices in summarizing productivity in simple data points while actually negatively impacting the work environment with the constant threat of surveillance.

On the other hand, the ubiquity of surveillance mechanisms, e.g., cameras in every smartphone, in smart doorbells, and as police bodycams, can also lead to “sousveillance,” i.e., citizens holding government agencies accountable for their actions.

In the context of digital humanism, the main tensions between surveillance and privacy arise because surveillance involves the collection of information, while privacy involves the protection of that information and control over how it is used. Surveillance can infringe on an individual’s right to privacy if it is conducted without their knowledge or consent, or if it involves the collection of sensitive or personal information. However, it can (and needs to) be designed to prevent abuses of power, minimize the collection of personal information, and protect individuals’ privacy, while still providing important security benefits to society. Still, surveillance is frequently seen as an “easy” and convenient solution without critical reflection about its benefits versus its harms, as evidenced by continuing efforts of implementing technology backdoors that undermine security and privacy, as well as eroding trust in technology. Thus, it is important to guarantee transparency, oversight, and accountability during the complete lifecycle of any technology, starting from how potentially privacy-invasive mechanisms are designed, over how they are deployed, to how the collected data is used.

## **2 Basic Concepts and Basic Definitions**

Surveillance refers to the monitoring or observation of people, places, including physical and digital surveillance. Classic physical surveillance includes the use of cameras in public spaces, historically known as closed-circuit television (CCTV) cameras, and physical tracking devices. The data collected through physical surveillance can also be augmented with technology, for example, with facial recognition mechanisms that augment the feed from surveillance cameras. Digital surveillance on the other hand includes monitoring online activity and communication, including emails, web browsing, and social media use. In addition to a categorization based on the technological means deployed to implement surveillance, it can also be differentiated along the following dimensions: covert vs. overt surveillance depending on whether it is conducted in secret and without the knowledge or consent of the individuals being monitored; mass vs. targeted surveillance depending on whether a large group of people is being monitored compared to only specific individuals or groups that are suspected of wrongdoing; and private vs. state surveillance depending on whether it is performed by companies or individuals, potentially for commercial purposes, or by the government and its agencies.

Demonstrating again the tension between surveillance and privacy (and the complexity of the term privacy) are the definitions of privacy according to the National Institute of Standards and Technology (NIST, 2023):

- “Assurance that the confidentiality of, and access to, certain information about an entity is protected.”
- “Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.”
- “The right of a party to maintain control over and confidentiality of information about itself.”

The following terms are frequently used to describe the negative effects surveillance and privacy-invasive technology can have, as well as users’ attitudes and behavior toward their privacy (Gerber et al., 2018):

- **Chilling Effect:** While the deployment of surveillance technology, such as cameras, can discourage harmful behavior, such as theft or crime, it also has negative effects on users’ exercising their legitimate rights. When faced with digital surveillance, for example, users might change their online behavior and self-censor instead of exercising their right to free speech.
- **Privacy Paradox:** Users’ online behavior often deviates from their values when it comes to protecting their private information, sometimes simply because the more privacy-invasive option is more convenient.
- **Privacy Calculus Theorem:** Users’ intention to disclose personal information is frequently based on a risk-benefit analysis as a trade-off between the functionality and the efficacy of a piece of technology and the data they need to share.

It is also important to note the diversity and type of data points that fall under the umbrella “private information:”

- **Personally Identifiable Information (PII):** Any type of information that can be used to identify an individual. PII can contain direct identifiers (e.g., passport information, social security number) that can identify a person uniquely or quasi-identifiers (e.g., gender, race) that can be combined with other quasi-identifiers (e.g., date of birth) to successfully recognize an individual. In addition to textual information, in particular, photos (e.g., selfies) are a valuable piece of PII that is collected and sold to train facial recognition software.
- **Device Identifiers:** Hardware- and software-specific identifiers can serve as the digital “license plate” of a device and form a specific type of PII that not necessarily contains private user data but nevertheless can be used to track their online activity. Besides fixed identifiers, such as IP and MAC addresses, or information from a phone’s SIM card, these identifiers can be generated through a process called “browser fingerprinting.” Important to note here is that these identifiers or fingerprints can also be useful for security purposes, for example, for a banking website to recognize suspicious logins and prevent account hacking. From a privacy perspective, one aspect is important though: whether those

identifiers are resettable by the user, or not. In the latter case, they provide means to track a user over the lifetime of their physical device without any control over them.

- **Metadata:** Even when full communication details, such as the content of emails and chats, are not available, the fact that two parties are communicating (when? for how long?) can be sensitive information.

Any of the above data may be collected for legitimate services, e.g., to protect users or provide more tailored services but also for secondary use cases, such as targeted profiling. Privacy issues arise in particular when users consent to sharing information with the first party, such as the developer of an app, but have no insight or control over whether the data is shared with other parties, such as advertisers and data brokers. Furthermore, while individual data points seem innocent enough, and users might think they “have nothing to hide,” the combination of information (from different sources) can reveal intimate details and personality traits users might not be aware of, a concept nicely illustrated by the “data onion” (Szymielewicz, 2019). In reality, research has found users to be profiled into 650,000 both highly specific and partly invasive categories (or “advertisement segments”) that can be used to target them (Keegan & Eastwood, 2023).

### 3 Methods

Similar to the variety of privacy threats and private information to be protected, there are a multitude of measures that can be taken either by individuals, app and service developers, corporations, or governments to protect privacy that include technical, organizational, and political aspects. Overall, a combination of these measures is needed to protect privacy effectively, but their application depends on the specific context and the involved privacy risks.

- **Privacy by Design:** Privacy should be a requirement and important factor from the inception of a product or service, i.e., built in from the beginning.
- **Privacy by Default:** Configurable settings should enable the most privacy-friendly ones by default, following the principle of “opt-in” to data collection rather than “opt-out.”
- **Privacy Preserving or Enhancing:** Users’ PII can be handled in a way that protects it while still maintaining the same level of functionality of an app or service compared to one with full (unprotected) access to PII.

#### Technical Measures

- **Access Controls:** Mechanisms that restrict access to sensitive information to authorized parties only. They can include password protection, multifactor authentication, or other forms of identity verification.
- **Encryption:** The process of encoding or transforming information in a way that it can only be read by authorized parties who possess a cryptographic key or

password. By encrypting data, users can ensure that it cannot be intercepted or read by unauthorized parties, ranging from people using the same public Wi-Fi in a coffee shop to Internet service providers (ISPs) and government agencies. A de facto standard for protecting communication through encryption is the use of the hypertext transfer protocol secure (HTTPS) instead of plain HTTP when visiting websites. Other examples include the encryption of emails, or the use of secure, i.e., end-to-end encrypted, messaging apps such as Signal. Other examples of encryption in action are virtual private networks (VPNs), which create a secure, encrypted connection (often also referred to as a “tunnel”) between devices, e.g., a user’s mobile phone and the Internet, or Tor, software that routes Internet traffic through a series of encrypted relays, making it difficult for anyone to track users’ online activities and allows users to browse the Internet near anonymously.

- **Anonymization:** The process of removing personally identifiable information from data sets to protect individuals’ privacy. A weaker form is pseudonymization, which processes personal data in a way that it can no longer be attributed to a specific user (without additional information). However, research repeatedly shows the difficulties in implementing such a process, and assumptions about what information would be necessary to de-anonymize users are typically too strong and broken in practice (Narayanan & Shmatikov, 2008; Deußner et al., 2020).
- **Data minimization and granularity:** Given the abovementioned difficulties in implementing privacy from a technical perspective, one important question remains: What kind of data is really necessary to provide a service or application? Can data be blurred, e.g., is the exact location necessary for a restaurant recommendation or does the city suffice? The best way to protect data typically is not to collect it at all.

### Organizational Measures

- **Privacy policies:** Statements that outline an organization’s data handling practices and the rights of individuals whose data is collected. They can provide transparency and accountability and help individuals make informed decisions about their data.
- **Employee training:** Raising awareness of privacy risks and best practices within an organization can help to prevent accidental or intentional privacy breaches by employees. The fact that ultimately humans often still access and handle collected information is not that obvious, for example, given the advances in automated audio and video processing. However, reports have shown how manufacturer’s employees can have unrestricted access to security cameras (Harwell, 2020), or employees and contractors still are transcribing voice messages (Frier, 2019) and smart speaker prompts.
- **Privacy impact assessments:** Systematic evaluations of the potential privacy risks of new or modified processes, systems, or technologies can help organizations identify and address privacy risks before they occur.



## Political Measures

- **Data protection laws:** Legal frameworks that regulate the collection, storage, and use of personal data can provide individuals with legal rights, such as the right to access, correct, or delete their data, and impose penalties for noncompliance or misuse.
- **International agreements:** Legal frameworks such as the General Data Protection Regulation (GDPR) in the European Union (EU) and collaborations like the EU-US Data Privacy Framework can help to establish global privacy standards and facilitate cross-border data protection.
- **Advocacy and activism:** Raising awareness of privacy risks is important to hold organizations and governments accountable for their privacy practices, as well as shape public policy to promote privacy rights and protections.

### *Example: General Data Protection Regulation (GDPR)*

The General Data Protection Regulation (GDPR) is a privacy law that was enacted by the European Union (EU) in 2018 (European Commission, 2016). The purpose of the GDPR is to give individuals more control over their personal data and to ensure that organizations are handling that data responsibly. One of its key aspects is the notion of consent: organizations are required to obtain clear and explicit consent from individuals before collecting and processing their personal data. It further gives individuals the rights to information about how their data is collected and handled, as well as the right to revoke consent and request the deletion of their data. It is an important piece of legislation that seeks to protect individuals' privacy rights and ensure that organizations are handling personal data responsibly. Similar regulations in other jurisdictions include (but are not limited to) the California Consumer Privacy Act (CCPA), the Brazilian General Data Protection Law (LGPD), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and the UK's Data Protection Act 2018 (DPA).

### *GDPR Consequence: Privacy Policies (and Labels)*

One mechanism that is frequently cited as a way for users to determine how their data is used and shared are terms of services and privacy policies. However, as a long line of research has shown, not only are privacy policies hard to understand for nonlegal experts, requiring at least university-level reading skills (Litman-Navarro, 2019), it is also practically infeasible for users to read the privacy policies of all apps and services they are using: A study in 2008 (McDonald & Cranor, 2008; Madrigal, 2012) estimated that individuals would spend 76 working days per year to read the privacy policies of every website they are visiting. Given the increasing complexity of policies (Lovato et al., 2023; Adhikari et al., 2023), partially due to legislative requirements, this number is clearly a lower bound.


An interesting proposal to condense the information from privacy policies and present them in a standard and easy to understand way are privacy nutrition labels (Kelley et al., 2009; Emami-Naeini et al., 2020) (see also Fig. 1 for an example). Recent developments by the two main mobile platform providers, Apple and Google, implement such a mechanism: Apple introduced App Store Privacy Labels in 2020, and Google introduced the Google Play Data Safety Section in 2021. Still,

## Security & Privacy Overview

Smart Security Camera NS200  
Firmware version: 2.5.1 - updated on: 6/15/2019  
The device was manufactured in: United States


Casa





---

  
**Security Mechanisms**

<b>Security updates</b>	Automatic - Available until at least 1/1/2022		
<b>Access control</b>	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed		

---


  
**Data Practices**

<b>Sensor data collection</b>	 <b>Visual</b>	 <b>Audio</b>	 <b>Physiological</b>	 <b>Location</b>
<b>Sensor type</b>	Camera	Microphone		
<b>Purpose</b>	Providing device functions, Research	Providing device functions, Research		
<b>Data stored on device</b>	Identified	Identified		
<b>Data stored on cloud</b>	Identified - Option to delete	Identified - Option to delete		
<b>Shared with</b>	Manufacturer, Third parties	Manufacturer, Third parties		
<b>Sold to</b>	Not sold	Not sold		

**Other collected data** Movement, Account info, Payment info, Device setup info, Device tech info, Device usage info

**Privacy policy** [www.NS200.example.com/policy](http://www.NS200.example.com/policy)

---

  
**More Information**

**Detailed Security & Privacy Label:**  
[www.iotsecurityprivacy.org/labels](http://www.iotsecurityprivacy.org/labels)




Fig. 1 Example of condensing information from privacy policies into a “nutrition label” (Emami-Naeini et al., 2020)

while these developments seemingly increase transparency, there is a lack of enforcement and accountability as this information is almost entirely self-reported by developers. Google offers the option to have part of this information independently validated, yet this mainly concerns whether an app adheres to security standards and best practices and not necessarily how it handles PII.

More generally, the notion of consent itself is up to debate. Service providers use “dark patterns” to elicit consent to data collection from users by the path of least resistance, leading to current approaches being termed as a “consent theater” (Fassl, 2021).

### **Emerging Privacy-Enhancing Technologies**

In addition to the safeguards individuals can take to protect their personal information and online activities, technology itself can be designed and deployed in a way that it is privacy-preserving or even enhancing.

*Homomorphic encryption* is a relatively new and still developing technology, and while there have been significant advances in recent years, it is not yet widely deployed in real-world applications. It is a type of encryption that allows computations to be performed on encrypted data without first decrypting it. This has the potential to greatly enhance privacy and security, as it would allow sensitive data to be processed and analyzed without ever being exposed in its unencrypted form. Still, it is a relatively complex and computationally intensive technology, and there are still challenges to be addressed in terms of its efficiency and scalability. There are also challenges for its practical implementation as existing software and hardware systems need to be modified to support it.

*Differential privacy* is a privacy-preserving technology that works by adding noise to data to mask individual records, thus preventing the identification of specific individuals while still allowing for useful analysis of the data. It has already been deployed in a number of real-world applications, most notably the US Census Bureau, Google in services such as Google Maps and Chrome, and Apple across MacOS and iOS. Still, there are also open research questions to improve its efficiency and scalability, as well as effectiveness in real-world settings.

*Synthetic data* is another promising approach that generates data with the same statistical properties and patterns of the original data while not containing any identifiable information of individuals. In addition to not exposing any private information by design, it can also augment existing datasets to make them more diverse and generalizable.

*Federated learning* is a machine learning technique where data is trained across multiple devices or systems without transferring the data to a central server, thereby preserving data privacy.

*Secure multiparty computation* allows multiple parties to compute a function or analyze data without revealing their individual inputs or data.

## **4 Critical Reflection**

While surveillance can be used for legitimate purposes such as crime prevention, it can also be abused and lead to negative consequences for individuals and society as a whole. Therefore, it is important to carefully consider the balance between privacy and security and ensure that surveillance is conducted in a transparent, accountable, and ethical manner. Surveillance is often seen critically or problematic for several reasons, including:

- **Invasion of Privacy:** It can violate individuals' right to privacy. On the one hand, the feeling of being watched or monitored can feel intrusive and uncomfortable. On the other hand, this can also have a chilling effect on free expression and association, making people more cautious and less likely to express dissenting views.
- **Abuse of Power:** Governments and corporations can use surveillance to gather information on individuals, track their movements and activities, and use that information to exert influence or pressure. Thus, it can be used as a tool for those in positions of power to control and manipulate others.
- **Discrimination and Targeting:** Surveillance can be used to unfairly target and discriminate against certain groups based on their race, ethnicity, religion, sexual preferences, health conditions, or political beliefs, potentially leading to harassment, persecution, or even violence.
- **Lack of Transparency and Accountability:** When conducted without proper oversight, surveillance can lead to abuses and violations of human rights. Furthermore, when conducted in a covert manner, i.e., the individuals being monitored have no idea that they are being watched, there is no way for them to hold the surveilling party accountable.

We have already seen examples of mass surveillance being implemented using questionable and controversial technical means.

Encryption backdoors are deliberate vulnerabilities or weaknesses built into encryption software or hardware, which allow authorized parties to bypass or circumvent the encryption and gain access to the protected information. Law enforcement and national security agencies see it as a useful tool to catch criminals or terrorists, frequently citing national security concerns and the need to catch pedophiles as ways to squash counterarguments. However, these backdoors undermine the very purpose of encryption, which is to protect sensitive information and communications from unauthorized access. It is naïve to assume they can be exploited only by authorized parties (and that criminals will not find more sophisticated technical means to circumvent to hide their tracks). On the contrary, they also provide effective targets for malicious actors, including hackers, cybercriminals, and foreign governments. Furthermore, while calling for more technical surveillance measures, the technical capabilities and human resources to even leverage existing technical means existing data sources are still lacking (Landau, 2016, 2017).

For example, the federal trojan (“Bundestrojaner”) is a term used to refer to a type of Trojan horse malware that was reportedly used by the German Federal Criminal Police Office (Bundeskriminalamt or BKA) to conduct surveillance on individuals suspected of criminal activities. The Bundestrojaner was first publicly acknowledged in 2011 when it was reported that the BKA had used the malware to conduct surveillance on a suspected terrorist. The malware was allegedly designed to be installed on a suspect's computer or mobile device, where it would then monitor their activity and collect data, including keystrokes, web browsing, and audio and video recordings. Unfortunately, it is by far not the only example of government-sponsored malware; other countries similarly toyed with the idea of developing (or simply buying) their own version of spyware.

In general, any backdoors, trojan horses, or other spyware can fundamentally undermine the trust that users have in technology, with serious consequences for individual privacy, as well as for businesses and governments that rely on technological means, such as encryption, to protect sensitive data. Thus, they warrant a critical debate about the appropriate balance between national security concerns and individual privacy rights.

Finally, similar to the “chilling effect” of individuals self-censoring their behavior online under the perceived threat of surveillance, citizens might behave differently when they know they are being watched by public cameras (Price, 2017).

## 5 Conclusions

In this chapter, we pointed out the inherent tension between surveillance and privacy. Surveillance mechanisms need to be designed in a way that they provide (physical) safety to society but also respect human’s right for privacy, as well as transparency, oversight, and accountability.

Legislation, such as GDPR, has already been successful in providing more transparency in how data is collected and used, but this solution is far from perfect: not only is it infeasible to read all privacy policies we encounter on a daily basis; how they can be enforced and whether the provided information is actually accurate is still an open question.

Privacy should be built into technology from the outset, through a design approach called “privacy by design.” This involves considering privacy implications at every stage of the design process and incorporating privacy protections as a fundamental aspect of the technology itself.

We also presented technological developments, such as homomorphic encryption and differential privacy, trying to address privacy issues, but there still is room for improvement to make them practical and deployable at scale.

As a final point, the threat of surveillance and lack of privacy severely impact users’ trust in technology and hinder its adoption. One great example for this was the development (and failure) of contact tracing mechanisms during the COVID-19 pandemic: while its deployment could have been an effective means to limit the spread of the disease, public mistrust limited its adoption and rendered any efforts in this direction irrelevant.

### Discussion Questions for Students and Their Teachers

1. What are acceptable tradeoffs between surveillance and privacy, where do you draw the line?
2. Do you recognize instances of the privacy paradox in your own behavior?
3. Think about the data you share online and the information that could be derived from them (see also the “data onion”) (Szymielewicz, 2019). Who would you be comfortable sharing this information with? How could this be (mis)used against you? By whom?

4. What do you think are the most effective privacy-protecting measures (technical, organizational, political)? In which context?
5. Can you think of further privacy-enhancing measures that could be designed?
6. Bonus: Take an online privacy test (Blue, 2015). Was there information that surprised you, and are you willing to share your impressions?

### Learning Resources for Students

On protecting your privacy in general:

1. Zotzmann-Koch, K. (2022) *Easy Ways to Be More Private on the Internet (Second Edition)*. edition sillbenreich.

On how to (and why) protect your privacy as part of particularly vulnerable groups:

1. Blue, V. (2015) *The Smart Girl's Guide to Privacy: Practical Tips for Staying Safe Online*. No Starch Press.
2. Lewis, S. J. (2017) *Queer Privacy. Essays From The Margins Of Society*. Mascherari Press.

On privacy policies and their evolution:

1. Adhikari, A. and Das, S. and Dewri, R. (2023) 'Evolution of Composition, Readability, and Structure of Privacy Policies over Two Decades' in *Proceedings on Privacy Enhancing Technologies (PETS)*. <https://doi.org/10.56553/popets-2023-0074>
2. Lovato, J. and Mueller, P. and Suchdev, P. and Dodds, P. (2023) 'More Data Types More Problems: A Temporal Analysis of Complexity, Stability, and Sensitivity in Privacy Policies' in *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT)*. <https://doi.org/10.1145/3593013.3594065>

On the inadequacy of privacy policies and alternatives:

1. McDonald, A. M. and Cranor, L. F. (2008) 'The Cost of Reading Privacy Policies' in *I/S: A Journal of Law and Policy for the Information Society*, 4(3).
2. Emami-Naeini, P. and Agarwal, Y. and Cranor, L. F. and Hibshi, H. (2020) 'Ask the Experts: What Should Be on an IoT Privacy and Security Label?' in *Proceedings of the IEEE Symposium on Security & Privacy (S&P)*. <https://doi.org/10.1109/SP40000.2020.00043>

On the mechanisms behind targeted advertisements and why companies try to "game" the system:

1. Hoofnagle, C. J. and Soltani, A. and Good, N. and Wambach, D. J. and Ayenson, M. D. (2012) 'Behavioral Advertising: The Offer You Cannot Refuse' in *Harvard Law & Policy Review*, 273.

On the topic of informed consent and why it is failing users:

1. Fassel, M. and Gröber, L. T. and Krombholz K. (2021) ‘Stop the Consent Theater’ in *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems (CHI EA)*. <https://doi.org/10.1145/3411763.3451230>

On why users behave contrary to their own privacy preferences:

1. Gerber, N. and Gerber, P. and Volkamer, M. (2018) ‘Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior’ in *Computers & Security*, 77. <https://doi.org/10.1016/j.cose.2018.04.002>

On the tension between surveillance capabilities and requests for more:

1. Landau, S. (2016) ‘The real security issue of the iPhone Case’ in *Science*, 352(6292). <https://doi.org/10.1126/science.aaf7708>
2. Landau, S. (2017) *Listening in: Cybersecurity in an insecure age*. Yale University Press.

## References

- Adhikari, A., Das, S., & Dewri, R. (2023). Evolution of composition, readability, and structure of privacy policies over two decades. In *Proceedings on Privacy Enhancing Technologies (PETS)*. <https://doi.org/10.56553/popets-2023-0074>
- Blue, V. (2015). *The smart girl's guide to privacy: Practical tips for staying safe online*. No Starch Press.
- Calacci, D., & Stein, J. (2023). From access to understanding: Collective data governance for workers. *European Labour Law Journal*, 14(2). <https://doi.org/10.1177/20319525231167981>
- Deußer, C., Passmann, S., & Strufe, T. (2020). Browsing unicity: On the limits of anonymizing web tracking data. In *Proceedings of the IEEE symposium on security & privacy (S&P)*. doi:<https://doi.org/10.1109/SP40000.2020.00018>
- Emami-Naeini, P., Agarwal, Y., Cranor, L. F., & Hibshi, H. (2020). Ask the experts: What should be on an IoT privacy and security label? In *Proceedings of the IEEE symposium on security and privacy (S&P)*. doi:<https://doi.org/10.1109/SP40000.2020.00043>
- European Commission. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)*. European Commission.
- Fassel, M., Gröber, L. T., & Krombholz, K. (2021). *Stop the consent theater*. In *Extended Abstracts of the ACM Conference on Human Factors in Computing Systems (CHI EA)*. <https://doi.org/10.1145/3411763.3451230>
- Frier, S. (2019). Facebook paid contractors to transcribe users' audio chats. *Bloomberg Technology News*, August 13 [online]. Available at: <https://www.bloomberg.com/news/articles/2019-08-13/facebook-paid-hundreds-of-contractors-to-transcribe-users-audio#xj4y7vzkg> (Archived: <https://archive.ph/66qcd>).
- Gellman, B., & Lindeman, T. (2013). Inner workings of a top-secret spy program. *Washington Post*, June 29 [online]. <https://web.archive.org/web/20170830105407/https://apps.washingtonpost.com/page/national/inner-workings-of-a-top-secret-spy-program/282/>.

- Gellman, B., & Poitras, L. (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *Washington Post*, June 7 [online]. Available at: [https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497\\_story.html](https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html) (Archived: <https://archive.is/ucSTd>).
- Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers and Security*, 77. <https://doi.org/10.1016/j.cose.2018.04.002>
- Greenwald, G., & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. June 7 [online]. Available at: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> (Archived: <https://archive.is/haGGj>).
- Harwell, D. (2020). Ring has terminated employees for abusing access to people's video data, Amazon tells lawmakers. *Washington Post*, January 8 [online]. Available at: <https://www.washingtonpost.com/technology/2020/01/08/ring-has-terminated-employees-abusing-access-peoples-video-data-company-tells-lawmakers/> (Archived: <https://archive.is/uwXJ4>).
- Hoofnagle, C. J. (2003). Big brother's little helpers: How ChoicePoint and other commercial data brokers collect and package your data for law enforcement. *North Carolina Journal of International Law*, 595.
- Hoofnagle, C. J., Soltani, A., Good, N., Wambach, D. J., & Ayenson, M. D. (2012). Behavioral advertising: The offer you cannot refuse. *Harvard Law and Policy Review*, 273.
- Kantor, J., & Sundaram, A. (2022). The rise of the worker productivity score. *The New York Times*, August 14 [online]. Available at: <https://www.nytimes.com/interactive/2022/08/14/business/worker-productivity-tracking.html> (Archived: <https://archive.is/2EaSk>).
- Keegan, J., & Eastwood, J. (2023). From "heavy purchasers" of pregnancy tests to the depression-prone: We found 650,000 ways advertisers label you. *The Markup*, June 8 [online]. Available at: <https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-depression-prone-we-found-650000-ways-advertisers-label-you> (Archived: <https://archive.is/1YgzN>).
- Kelley, P. G., Bresee, J., Cranor, L. F., & Reeder, R. W. (2009). A "nutrition label" for privacy. In *Proceedings of the USENIX symposium on usable privacy and security (SOUPS)*. doi:<https://doi.org/10.1145/1572532.1572538>.
- Knockel, J., Parsons, C., Ruan, L., Xiong, R., Crandall, J., & Deibert, R. (2020). *We chat, they watch how international users unwittingly build up wechat's Chinese censorship apparatus*. Technical Report, CitizenLab. Available at: <https://citizenlab.ca/2020/05/we-chat-they-watch/>.
- Landau, S. (2016). The real security issue of the iPhone Case. *Science*, 352(6292). <https://doi.org/10.1126/science.aaf7708>
- Landau, S. (2017). Listening. In *Cybersecurity in an insecure age*. Yale University Press.
- Litman-Navarro, K. (2019). We read 150 privacy policies. They were an incomprehensible disaster. *The New York Times*, June 12 [online]. Available at: <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html> (Archived: <https://archive.is/rPZGn>).
- Lovato, J., Mueller, P., Suchdev, P., & Dodds, P. (2023). More data types more problems: A temporal analysis of complexity, stability, and sensitivity in privacy policies. In *Proceedings of the ACM conference on fairness, accountability, and transparency (ACM FAccT)*. doi:<https://doi.org/10.1145/3593013.3594065>.
- Madrigal, A. C. (2012). Reading the privacy policies you encounter in a year would take 76 work days. *The Atlantic*, March 1 [online]. Available at: <https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/> (Archived: <https://archive.is/2ER6B>).
- McDonald, A. M., & Cranor, L. F. (2008). The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4(3).
- Narayanan, A., & Shmatikov V. (2008). Robust De-anonymization of large sparse datasets. In *Proceedings of the IEEE symposium on security and privacy (S&P)*. doi:<https://doi.org/10.1109/SP.2008.33>.



- National Institute of Standards and Technology (NIST). (2023). *Glossary: Privacy*. Available at: <https://src.nist.gov/glossary/term/privacy>
- Peck, D. (2013). 'They're watching you at work'. *The Atlantic*, December 15 [online]. Available at: <https://www.theatlantic.com/magazine/archive/2013/12/theyre-watching-you-at-work/354681/> (Archived: <https://archive.is/s4YJk>).
- Perlberg, S. (2014). Targeted ads? TV can do that now too. *Wall Street Journal*, November 2014 [online]. Available at: <https://www.wsj.com/articles/targeted-ads-tv-can-do-that-now-too-1416506504> (Archived: <https://archive.is/OaFA0>).
- Price, B. A., Stuart, A., Calikli, G., McCormick, C., Mehta, V., Hutton, L., Bandara, A. K., Levine, M., & Nuseibeh, B. (2017, June). *Logging you, logging me: A replicable study of privacy and sharing behaviour in groups of visual lifeloggers*. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technology 1, 2, Article 22. <https://doi.org/10.1145/3090087>
- Razaghpahan, A., Nithyanand, R., Vallina-Rodriguez N., Sundaresan, S., Allman, M., Kreibich, C., & Gill, P. (2018). Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. In *Proceedings of the annual network and distributed system security symposium (NDSS)*.
- Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018). How Trump consultants exploited the Facebook data of millions. *The New York Times*, March 17 [online]. Available at: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> (Archived: <https://archive.is/jKMM9>).
- Sherman, J. (2022). *Data brokers and data breaches* [online] Available at: <https://techpolicy.sanford.duke.edu/blogroll/data-brokers-and-data-breaches/> (Archived: <https://archive.is/pM5jy>).
- Szymielewicz, K. (2019). Your digital identity has three layers, and you can only protect one of them. *Quartz*, January 25 [online]. Available at: <https://qz.com/1525661/your-digital-identity-has-three-layers-and-you-can-only-protect-one-of-them> (Archived: <http://archive.today/vxQYF>).
- Tagliaro, C., Hahn, F., Sepe, R., Aceti, A., & Lindorfer, M. (2023). I still know what you watched last Sunday: Privacy of the HbbTV protocol in the European smart TV landscape. In *Proceedings of the annual network and distributed system security symposium (NDSS)*.
- Whittaker, Z. (2023) US intelligence confirms it buys Americans' personal data. In *TechCrunch*, June 2023 [online]. Available at: <https://techcrunch.com/2023/06/13/us-intelligence-report-purchase-americans-personal-data/> (Archived: <https://archive.is/nMXzH>).
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.

**Open Access** This chapter is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

