Is privacy possible in a digital world?

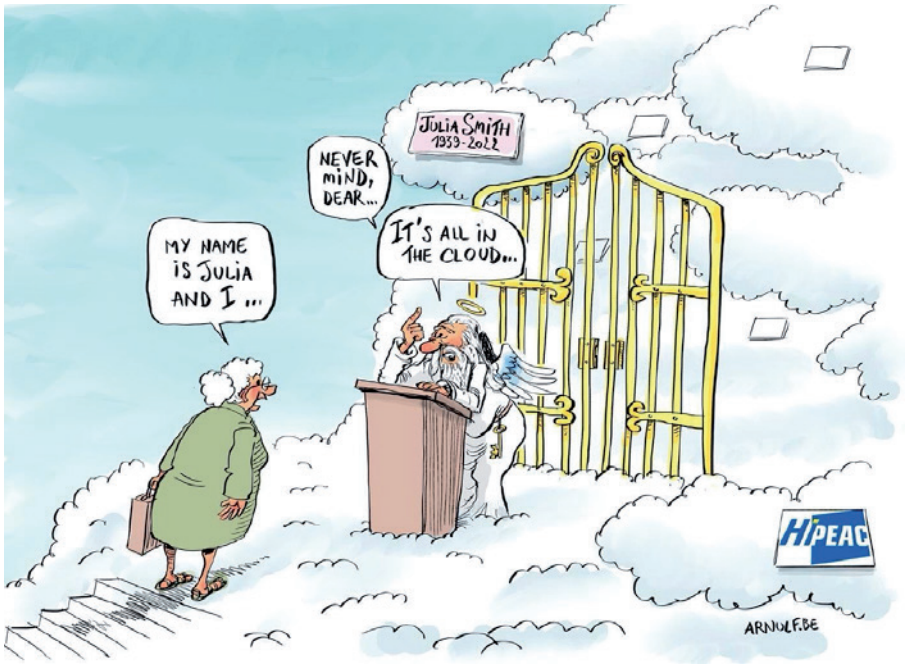
Bart Coppens, Olivier Zendra

There is growing awareness of the importance of privacy while, at the same time, we are sharing ever more private data with third parties. This creates an uneasy tension.

Is privacy possible in a digital world?

By BART COPPENS and OLIVIER ZENDRA

While privacy used to be a concern only for a limited number of people, in recent years awareness of it has been growing. This has been for a number of reasons, including the implementation of the General Data Protection Regulation (GDPR), the growing impact of data leaks, and data logging by governments and enterprises. In addition, there have been high-profile examples demonstrating how new legislation can turn seemingly innocuous private data against its owners. At the same time, the majority of us are consciously or unknowingly transmitting an increasing amount of private data to the cloud, which increases the likelihood of it being leaked or abused.



To try and reconcile these two opposing directions, both consumers and businesses should enhance their knowledge of privacy issues and their use of privacy-enhancing technologies, and enterprises should include privacy by design into their IT development processes.

Key insights

- Ever more data is being sent to and collected by governments and private companies alike.
- This data can then be analysed with big-data methods and artificial intelligence (AI), which has serious implications for privacy.
- The scope and volume of the data being collected and analysed is often not clear to consumers, who are sometimes even completely unaware that it is happening.
- However, there is increasing public awareness of privacy, not only of the fact that personal data is being collected, but also that it can be leaked, either on purpose or inadvertently.
- Technical solutions exist to improve privacy. The European Union (EU) has a role to play.

Key recommendations

- Promote research into technologies that enhance people's privacy and reduce the risks and impact of leaks of private data.
- Stand by EU principles of privacy for its citizens, requiring companies to actively adhere to the principles of privacy by design, and not allowing backdoors to be put into applications.
- To effectively enforce privacy, base information and communication technology (ICT) systems either on open-source software and hardware, or on EU-made, trustable because audited, proprietary hardware and software.
- Restrict how AI can be used to infer and reveal sensitive information from information which is seemingly less sensitive; or restrict the collection of such data.
- Invest in post-quantum cryptography so as to have EU-designed and EU-validated quantum-resistant encryption schemes.

We live in an era in which *almost everything we do is transmitted to servers beyond our control*. To give just a few examples, our private documents are stored in the cloud, while in some countries internet providers are legally obliged to keep track of which websites we visit [14]. Mobile service providers keep track of where our mobile phones make contact to their base stations and thus keep track of where we are; when we drive, our vehicle licence plates are captured by an increasing number of automatic number-plate recognition (ANPR) cameras which are placed for various purposes by governments and municipalities [15,16,17]. The list goes on. People even freely put microphone-based listening devices such as Amazon Echo [11], Apple Siri devices [12], Google Nest [13], etc. in their homes for purposes of convenience and comfort.

Sometimes, this sharing of information is quite intentional. When individuals share a document online, they expect that this information will be shared only with the intended recipients. What they do not usually realize is that others will also have access to this information. In fact, the document is stored on servers, which can be read by legitimate system administrators, teams that deal with abusive or illegal content that may be stored on that server, unrelated people through server misconfigurations, or hackers who gain access.

Moreover, as a result of the transition to cloud-based data storage and processing, data is often no longer held locally on the premises of the organizations to which we entrust our data, but is instead stored on infrastructure that is shared by several companies. Even if they deliberately choose to share information online, the majority of users are typically unaware of the extent to which it may be accessible to others. The amount of information gathered and stored which is *not* explicitly shared by users is orders of magnitude larger.

It is thus clear that privacy is an important topic that directly affects the lives of many people. In this article, we first discuss in more detail the kinds of **personal and private information** that nowadays are being generated, collected, and potentially leaked. We then describe some of the **technical and policy directions** that can help us to **protect** our **data and privacy** better.

Personal and private information

As a society, we are generating and storing an ever-increasing amount of (private) data. This includes (confidential) company information. Almost all of this data is delivered to and kept on cloud-based servers, regardless of its origin or whether this was done intentionally by a user. Although those of us who live in the EU should now be *informed about the fact that data is collected, most people are unclear about the scope of the increasing amount of data that is being collected, processed, and stored*. The scope of the data gathered takes on two dimensions: which data is actively gathered, and which *additional* data *can be inferred*. The trend towards a service-based cloud economy only exacerbates the scope to which this data is gathered and shared, and the risks to which this data is exposed.

All of this begs the question: what sort of personal and confidential data are we discussing? As previously indicated, there is the data that we create and upload ourselves. However, the data collected goes well beyond that, encompassing information pertaining to private conversations, gender, sexual orientation, race, date of birth, religion, political affiliation, medical data, and so on.

It is obvious that we do not want this type of information to be accessible to unrelated persons; yet this is precisely what happens. The online actions of individuals are tracked by advertising corporations such as Google and Meta in order to sell increasingly tailored advertisements [22,23]. On the basis of this information, data analysis and machine learning techniques are then used to develop a profile of personal interests, which is capable of deducing even sensitive information such as sexual orientation [28].

As part of so-called legitimate commercial objectives, this data is also traded and sold in the advertising industry [49]. Advertisers are interested in targeting extremely specific groups of individuals. Extreme instances include targeting individuals present at political demonstrations or individuals who routinely go to church [53]. This information can then be merged with other types of personal information, narrowing down the targeted population until it is possible to identify individuals. All of this information must be tracked and integrated in some way for such tailored advertising to be possible.

Some advertising companies go to quite some lengths to circumvent anti-tracking measures that are implemented by browsers [24]. Some totally unscrupulous companies even scrape the internet for people's pictures from different social media channels and other websites, in order to build and train very accurate facial recognition of these people without their consent [25]. These facial recognition engines can then be sold to governments and commercial organizations across the world [26,27]. This tracking of data has further ramifications with regards to sovereignty. US or Chinese companies keep track of the data of EU citizens, harvest their pictures and process this data abroad, outside EU laws and regulations; this can create problems that are hard to address and solve.

In theory, the GDPR requires explicit consent to be given when private information is kept of users. However, people quickly grow tired of cookie banners and information tracking pop-ups, and are trained to click on anything that allows them to consume their content faster. Furthermore, until recently, it was not clear that the same level of care needs to be taken when the tracked data in and of itself is not private, but when sensitive information can be deduced from it. For example, a recent case for the Court of Justice of the European Union tackled the following issue: keeping track of the name of someone's partner spouse allows one to deduce someone's *sexuality* [51]. And while the latter is clearly private information, it was not clear that the former was. However, the court ruled that, precisely because that inference is possible, the former is private information as well [51]. This is an important milestone, and should have far-reaching consequences.

How is it that all of this information, including sensitive information and information from which sensitive information might be deduced, is monitored in the first place? Obviously, there are countless sources. As previously indicated, people occasionally disclose information explicitly, for example to get access to content. However, much more common are inadvertent data disclosures. For instance, while we drive around, there are automatic number-plate recognition (ANPR) cameras everywhere, which aim to detect flagged vehicles or impose a maximum average speed limit along a road segment. In addition to these government-operated cameras, private residents are increasingly installing cameras as well, both security cameras and standard door cameras, such as those associated with Google Nest. As many of them are cloud-connected, not only do the owners of these cameras have access to the recordings, but also the corporations linked with these cameras, and they can potentially provide access to the police without a court order [55]. The latter mechanism, which may be necessary for efficient law enforcement, can be abused nonetheless by malevolent people to access information they should not have access to [59].

In the examples above, the cameras are highly visible. However, there are other examples where a device's role in compromising privacy is not so obvious. People are often astonished to learn that their listening gadgets not only send fragments of their private conversations to the device manufacturer, such as Amazon, but also to subcontractors who listen to them to improve the accuracy of the voice-recognition engines that power these devices [18]. The information regarding cell phone activities that is being tracked and stored is another example. This includes information about who is speaking with whom and for how long, as well as the location of individuals. This information can then be aggregated to get estimates of which locations are busier than others, and providers can sell this information [62].

Figure 1: A sign announcing camera surveillance at George Orwell Square in Barcelona [68].

Even when this information is *not* sold to others, it can still be problematic. Tesla vehicles, for instance, are fitted with a multitude of cameras and other sensors. Due to concerns that they could be used for espionage, Tesla vehicles have been barred from cities that host Chinese party leadership meetings and Chinese military installations [54,57]. In a recent lawsuit filed against Tesla by the father of a victim of a tragic car accident, Tesla supplied months of historical speed data in an attempt to transfer blame to the driver based on the fact that they had driven over the speed limit in the past [54]. Tesla maintains that it will not sell such information, but it may share it with third parties including business partners, service providers, and government agencies [58].

The ways in which companies track information can also be quite surprising. Information can even be deduced based on user behaviour. For example, when scrolling through a Facebook feed, Meta does not only keep track of which links a user clicks on, but also how long that user spends looking at certain items in their feed: do they scroll past them quickly, or do they linger on certain posts longer? This also allows Meta to deduce information about user likes and interests, even if these users don't explicitly provide them with this information [52].

There is thus a real issue surrounding privacy and awareness of privacy issues. While privacy has always had wide-reaching consequences for some groups of people and professions, ranging from LGBTQIA+ people to journalists who need to protect their sources [56], these consequences are also reaching ever more people.

One recent example is that of data related to abortions, in the wake of the US Supreme Court reversing its previous decision in the Roe v. Wade case and causing abortions to become illegal in several US states. What many people do not realize is that much data about abortions, again including data from which this can be *inferred*, is stored by a large number of (international) companies. Highly personal data such as text messages, emails, payment records, etc., which might merely *imply* that a user had an abortion is not only stored by companies, but can then also be accessed by authorities [43,45]. This includes data from apps which help women track their menstrual cycles [44,45], and if someone just *searches for* abortion pills online [45].

Companies tracking location data may find that this is suddenly a liability, as this information also includes visits to abortion clinics [46]. Some companies subsequently realized that storing as much data as possible about users might not have been the best idea, but still struggle to limit the scope of the captured data. For example, while they can try to simply remove (or not store) location data around abortion clinics, but this in and out of itself might not prove sufficient, as long as there enough location information is being kept from the neighbouring area. For example, in a related context, fitness tracking social networks allow users to enable endpoint privacy zones to hide the begin and end of tracks so as to hide the exact location of people's homes. However, creating schemes that prevent attackers from inferring these locations anyway turns out to be challenging and not necessarily user friendly [47]. Worse, even if people explicitly opt out from one kind of location data collection, there might be multiple systems independently collecting such data: Google recently settled a lawsuit over the fact that turning off the "location history" checkbox only stopped a Google Maps feature, not all Google location tracking [48].

In summary, *in addition to typical government-related activities, private companies are keeping track of increasingly more detailed information about people who are not even necessarily their users*. And even information which, at first glance, might not seem private in and of itself, can still lead to sensitive information being deduced from it.

Technical means to protect our data and privacy

Now, how can we effectively safeguard our data? The simplest answer would be to not have this data collected at all, and if it is collected to not share it at all: data that is not shared is really private data. However, the extent to which data is currently exchanged whenever we engage with today's predominantly digitized world makes this impractical unless people are willing to become (partial) digital and social recluses, so a middle ground needs to be found. This can be achieved at least in part by advocating and selecting technology that enhances our privacy, as opposed to ignoring it or, worse, deliberately trying to circumvent it.

In order to do so, we need to *design systems with privacy in mind from the ground up*. How a system handles private data and how it deals with privacy should be design requirements from the start. In 2010, the International Conference of Data Protection and Privacy Commissioners published a resolution encouraging recognition of the fact that privacy by design is an essential component of privacy protection, as well as the adoption of a set of foundational principles of privacy by design [29]. One of these principles is that privacy should be *embedded* in the design, and it should be an essential core of the functionality of the system [30]. These guiding principles were as true and necessary then as they are now.

For example, rather than sharing documents and messages with people where the shared data is stored in an unencrypted form on cloud servers, we can use solutions with true *end-to-end encryption*. Unlike Facebook Messenger, Signal [10] and the EU-based Olvid [9] encrypt the data such that intermediate servers cannot decipher the message[1]. While FaceBook Messenger supports end-to-end encrypted chats, this is not yet the default policy; users have to manually enable this function, and, if they don't, Meta still has access to the plain-text versions of the messages [60].

Where true end-to-end communications are not possible, or where people risk being tracked, it would still be beneficial to at least choose a *technology or solution which explicitly focuses on the privacy of its users*, like for example the EU-based Qwant search engine [31], or the Brave browser [32], that put an emphasis on protecting their users' privacy. Of course, in the case of a communications app, there needs to be a critical mass of people using it: there seems little point switching to an app for communicating with friends and family if they do not migrate. On the contrary: one is then stuck with two apps instead of one app: an app to communicate securely with a few people who have migrated, and an app to communicate with the rest. The EU should encourage more initiatives and further developments and investments into such privacy-aware technologies and companies, and encourage the adoption of these technologies, possibly mandating them in its own services, to help protect its citizens and its sovereignty over data.

Of course, a simple and effective way to have fewer problems with private data potentially being compromized is to not send it over the network at all. One way in which this can be solved is by ensuring that most or even all computations that normally take place in the cloud now take place locally, with the *processing being done at the edge*. This also has implications for industrial applications in the context of the internet of things (IoT) and cyber-physical systems (CPS): the more data is processed in those devices themselves, rather than having to be transmitted to cloud servers for processing, the less private data can be abused or leaked. A fog or federation of local devices sharing part of the global information in an encrypted way could solve the problem of accessing larger computing or storage resources in a more local manner.

If data does need to be transmitted or computed remotely, it is important to do this in a secure fashion that preserves as much security and privacy as possible. Most companies already try to *protect most sensitive data at rest and in transit with encryption*, for example with the Advanced Encryption Standard (AES) and Transport Layer Security (TLS). However, this data still needs to be processed, for which the data is currently still decrypted (and thus unprotected) on the systems that process it.

Furthermore, if this data processing involves the data being searchable or queryable in a database, many systems will still store this data in an unencrypted form. One way to mitigate this problem is to *do the data processing on encrypted data*, in such a way that the personally identifiable information (PII) is not known to the system performing the actual processing. Examples of such techniques are (fully) homomorphic encryption (FHE), which still requires research to decrease its computing resource requirements, and secure multi-party computation.

There are many fields in which homomorphic encryption would significantly increase the privacy of data in the context of cloud-based data processing. In the medical sector, users would be able to upload their ECG data and have a cloud provider monitor their health without actually sharing their data with that cloud provider [2]. Similarly, people would be able to have their genomes analysed by third parties without information being passed on about which genetic diseases they have or other PII such as gender, race, etc [3].

Modifying different cloud-based machine learning tasks to protect PII would also significantly reduce the risks associated with outsourcing the relevant data. For example, face verification or face recognition would no longer expose photographs of people [4], and performing optical character recognition would no longer leak the text being processed [5]. Furthermore, if the recognized text is from licence plates that need to be queried in a database of stolen and wanted vehicles, for example, one solution could be to prevent the processing of all licence plates from leak-

1 In addition, Olvid does not require you to provide your phone number, since it does not rely on any central directory.

ing information about *non-stolen* cars [6]. The EU should invest in more technologies such as these, so that if PII data does need to be processed, the amount of data that can be intentionally or inadvertently leaked is minimized as much as possible.

Given the urgency within today's business landscape to achieve more robust data privacy systems, we predict and advocate for an increase in the design and use of such homomorphic encryption and related techniques. Some start-ups already provide very specific applications of these techniques [7]. One limiting factor in applying FHE right now is its overhead. Both the time needed to process the data and the size of the messages that need to be exchanged with the cloud provider currently increase dramatically when FHE is applied. At present, this means that many of those techniques are unfortunately not yet usable in practice. In the meantime, some specific cases might not need to send the PII itself to third parties.

Another issue to take into account when protecting data by encrypting it is how resistant the encryption scheme is to the changing landscape of attackers' capabilities. One clear but constant change is the increase in the processing speed of computers. As one of the most obvious goals of an attacker is to recover the information, the question is how long information can remain private, and how this time decreases with an increase in processing speed, and by how much we then increase the strength of the encryption (for example, by increasing the key size) to compensate for this.

In the case of traditional computers, it is quite clear how these scaling laws work, and increases in computing power do not immediately threaten the security of data encrypted with traditional encryption schemes. However, when switching to the different computing paradigm of quantum computers, this is not necessarily the case, because certain algorithms are believed to run significantly faster on quantum computers than on traditional computers. With some algorithms, it is sufficient to choose larger key sizes to compensate for this. However, other algorithms could be completely broken with quantum computers. Such algorithms need to be replaced with algorithms that could withstand attacks from a quantum computer. This field is called post-quantum cryptography (which is sometimes abbreviated as PQC).

It is crucial that we begin defending not only against existing threats, but also against future threats. There are two compelling arguments for deploying post-quantum cryptography as soon as possible. First, the data we send or save now may remain confidential and valuable in the future, when potential adversaries may have access to quantum computers, so we should safeguard against future attacks.

Second, switching algorithms is not an instantaneous process; compatibility must be ensured across the board. While many devices may be upgraded quickly to support more algorithms, this is not always the case. Obviously, every new cryptographic algorithm must be extensively examined. One of the finalist algorithms in the NIST competition on post-quantum cryptography [66], for instance, was recently invalidated: researchers demonstrated that a standard laptop could crack it in less than an hour [64]. Therefore, it is clear that additional research into these algorithms is required. Additionally, switching algorithms should be done with caution. Google, for instance, recently opted to begin utilizing post-quantum cryptographic algorithms to secure its internal communications, but they ensured that this was an additional layer of security [65], rather than being the only one.

However, it is not sufficient to use state-of-the-art encryption algorithms to protect PII. Software that is not secure can still leak all kinds of confidential and private information to attackers, even if under normal circumstances this data is stored and transmitted securely. Some *security-related instruction set architecture extensions* have explicit implications for improving privacy. For example, one of the goals of Intel's Software Guard Extensions (SGX) is to protect the execution of certain code fragments from attackers that have control over the rest of the system, including the operating system itself. This can then be used to protect sensitive and private information even when the entire system is being attacked. However, the many recent attacks on SGX show that even this technology is clearly not yet mature enough to withstand such attacks in practice [19,20,21]. It may even be that the SGX model of allowing execution of code on private data, and general-purpose code execution by untrusted users, might not be feasible.

Protecting our data and privacy through policy

Thanks to *regulations such as the GDPR*, EU citizens should be better protected against at least some forms of unwanted processing of private data, and they should now at least be informed when such data

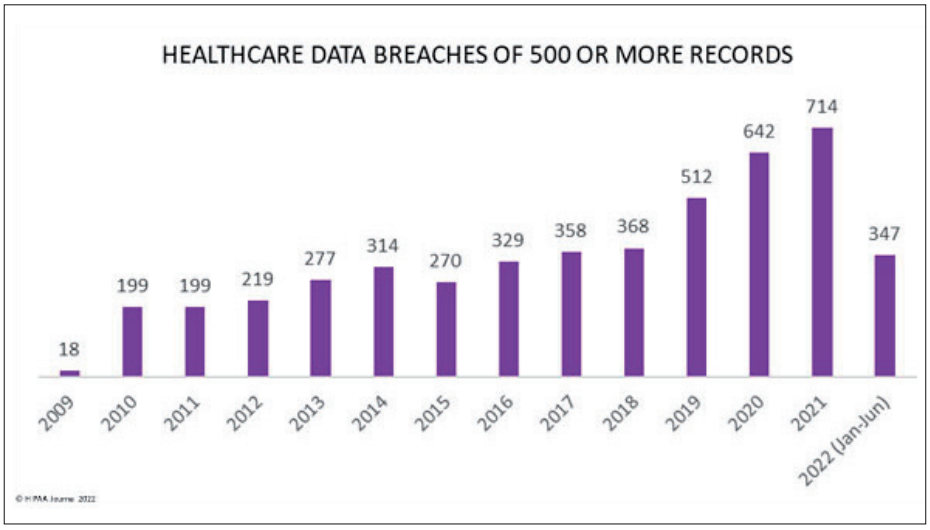


Figure 1: Reports of healthcare data breaches of 500 or more records reported to the US Department of Health and Human Services' Office for Civil Rights between 2009 and June 2022 [1].

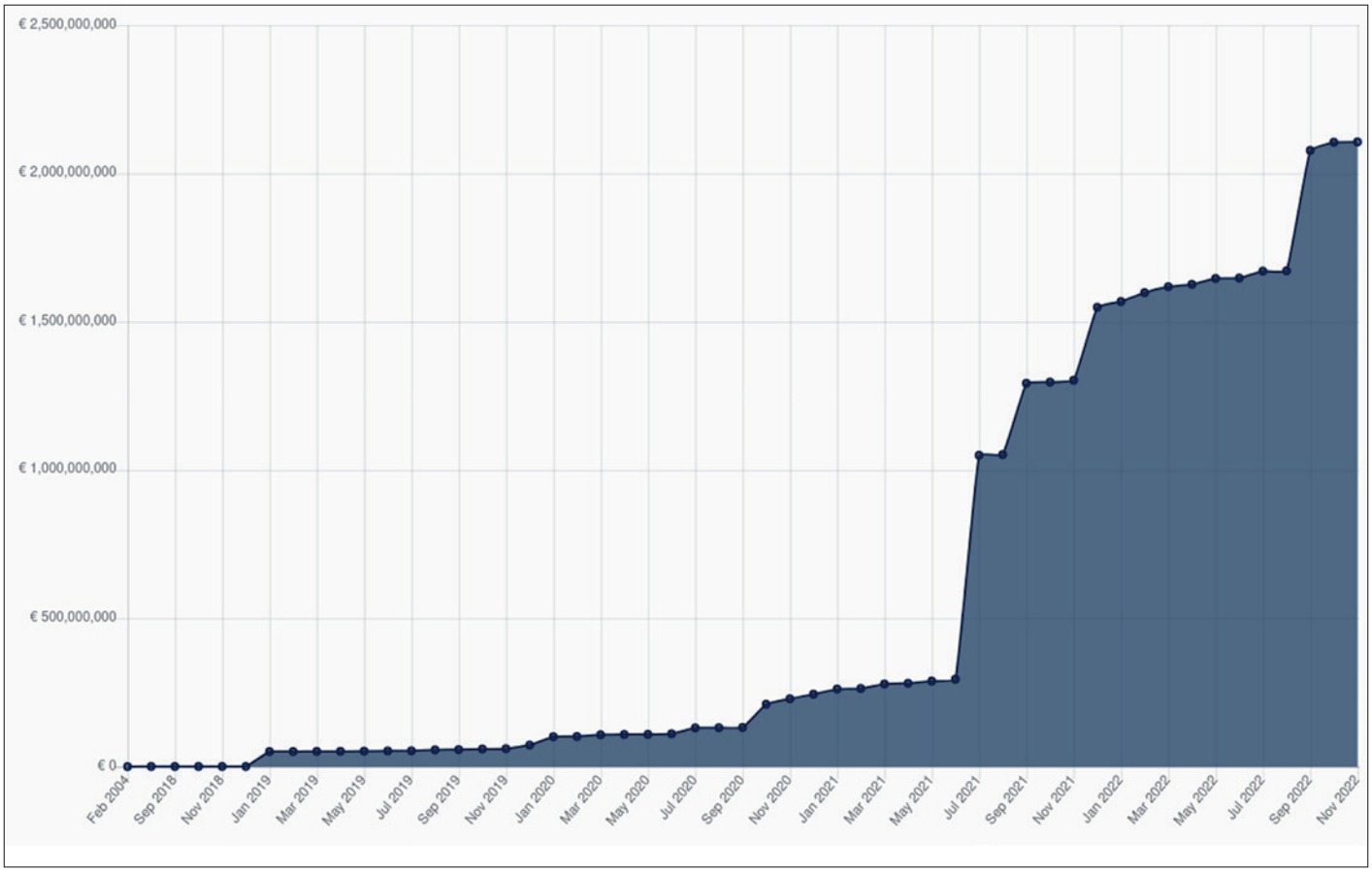


Figure 2: Cumulative sum of GDPR-related fines [63]

is leaked or mishandled. This represents huge progress in terms of the public being informed and aware of data protection issues and should be hailed as a very positive step. However, data leaks are still likely to be a problem. Figure 1 gives an idea of the scale of the problem, indicating healthcare data breaches of 500 or more records reported to the US Department of Health and Human Services' Office for Civil Rights between 2009 and June 2022. Unfortunately, rather than decreasing, the numbers are going up. Similarly, Figure 2 shows the cumulative sum of GDPR-related fines; again, the fines show no sign of decreasing.

In this context, it is important to stress the importance of the entire system being *secure and not weakened by backdoors*. Some governments have advocated for such backdoors in operating systems, telecommunications networks, and secure/encrypted communication platforms, so that only "they" may (legally) get access to systems and decode encrypted data. In 2020, the EU Council called for law enforcement to have access to encrypted private data [36], while in 2021, the Belgian government proposed sweeping new legislation mandating backdoors in encrypted communications networks [37]. This latter proposal was rescinded in response to public backlash and unfavourable feedback from experts and the Belgian Data Protection Authority [38].

Along these lines, Apple also proposed a new "feature" for iCloud in which an iPhone would check photographs for child abuse content. While this proposal appeared limited in scope, it met with a massive public outcry from both experts and civil rights organizations, who feared that it would open the door to massive government surveillance and transform mobile phones into permanent government spying devices, causing Apple to delay the release of this feature [43]. In exactly this context, though, the EU has again proposed to weaken their citizen's privacy and security [61], which we consider would be a highly insecure mistake.

A fundamental issue with these backdoors is that they reduce the security of the entire system [40,41,42]. There is in fact no guarantee that the law enforcement agents of the country will be the *only ones* with access to these backdoors: other countries and criminals might be able to use them too. For example, a pseudo-random number generator containing a weakness which had allegedly been introduced by the US National Security Agency (NSA) eventually found its way into firewalls, where it was exploited by unknown parties [34]. Some allege that Intel's closed-source management engine on chips not only supports well-intended remote management functions, but might also be used by other (malicious) parties to get remote access to machines [35].

Such backdoors decrease the security of individuals and their data. They also undermine the EU's efforts to protect the privacy and security of its residents by diminishing people's trust in computers and telecommunications infrastructure. Furthermore, such measures would affect the confiden-

tiality of company data, which would then be susceptible to leakage through these backdoors. Thus, to protect the privacy of its inhabitants and the secret information of its businesses, the EU should not even consider legalizing such backdoors.

However, while an insecure system can lead to information leaks, the converse is not necessarily true. A secure system cannot distinguish between purposeful leaks of information (for example, a user who wants to print his/her own bank statements), versus inadvertent leaks of information (for example, these bank statements being stored unencrypted on disk). One possible solution here is language-based information-flow security that allows programmers to explicitly define which flows of information are allowed, and to define properties on these flows [8].

A final source of leaking private information is the users themselves: frequently, they are unaware of the actual private information that can be extracted from the data being shared: posting pictures of someone in a bar or nightclub could be interpreted by an insurance company as evidence that the individual is a health risk because they drink alcohol. There are systems based on artificial intelligence that can analyse such public content and warn users about such "social" information [33].

In light of this, it would be useful to consider restricting which information can be collected and stored, and how data that can be inferred from it should be treated.

Conclusion

Public awareness of privacy issues is slowly increasing thanks to initiatives such as the enactment of the GDPR, which is widely considered as an outstanding and pioneering move on the part of the EU, but also with people seeing the impact of how seemingly innocent data collection can make them vulnerable to prosecution. These will hopefully be a trigger for people to think more about where and how their private data is being collected, stored, and used, which in many cases is anyplace, anytime, by most of the tools and applications. This will hopefully encourage individuals to be more vigilant about protecting their own privacy, as well as demanding more robust privacy protections from ICT companies.

The EU has a role in regulating, promoting, and supporting EU-based solutions that protect privacy and sovereignty. It should build on its position as a leader in privacy legislation, which has already had an influence on laws in other parts of the world [67]. If companies wish to sell ICT products and services in the EU, they should meet stringent EU-defined privacy requirements. Lastly, companies should be obliged to ensure privacy by design in their products and services.

References

[1] Healthcare Data Breach Statistics, HIPAA Journal, online, accessed November 22, 2022. https://www.hipaajournal.com/healthcare-data-breach-statistics/

[2] Kocabas, Ovunc, et al. "Assessment of cloud-based health monitoring using homomorphic encryption." 2013 IEEE 31st International Conference on Computer Design (ICCD). IEEE, 2013

[3] Miran Kim, Kristin Lauter, "Private genome analysis through homomorphic encryption", BMC Med Inform Decis Mak. 2015; 15(Suppl 5): S3.

[4] J.R. Troncoso-Pastoriza, D. González-Jiménez, F. Pérez-González, 2013. Fully private non-interactive face verification". IEEE Transactions on Information Forensics and Security, 8(7), pp.1101-1114

[5] Nathan Dowlin, Ran Gilad-Bachrach, Kim Laine, Kristin Lauter, Michael Naehrig, and John Wernsing. 2016. "CryptoNets: applying neural networks to encrypted data with high throughput and accuracy. In Proceedings of the 33rd International Conference on International Conference on Machine Learning – Volume 48 (ICML'16), Maria Florina Balcan and Kilian Q. Weinberger (Eds.), Vol. 48. JMLR.org 201-210.

[6] Sunil, Archana Bindu, Zekeriya Erkin, and Thijs Veugen. "Secure matching of Dutch car license plates." Signal Processing Conference (EUSIPCO), 2016 24th European. IEEE, 2016

[7] https://www.privatebiometrics.com/, accessed December 4, 2020

[8] A. Sabelfeld and A. C. Myers, "Language-based information-flow security", in IEEE Journal on Selected Areas in Communications, vol. 21, no. 1, pp. 5-19, Jan. 2003.

[9] Olvid. https://olvid.io/technology/en/

[10] Signal. https://signal.org/docs/

[11] Amazon Echo. https://en.wikipedia.org/wiki/Amazon_Echo

[12] Apple Siri. https://en.wikipedia.org/wiki/Siri

[13] Google Nest. https://en.wikipedia.org/wiki/Google_Nest_(smart_speakers)

[14] Judgments in Case C-623/17, Privacy International, and in Joined Cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others. Press release 123/20, Court of Justice of the European Union, 6 October 2020

[15] Automatic Number Plate Recognition, Police.uk https://www.police.uk/information-and-advice/automatic-number-plate-recognition/ accessed December 2020

[16] Denmark: Targeted ANPR data retention turned into mass surveillance EDRi, September 6, 2017, https://edri.org/our-work/denmark-targeted-anpr-data-retention-turned-into-mass-surveillance/

[17] Automatic number-plate recognition - Usage, Wikipedia, https://en.wikipedia.org/wiki/Automatic_number-plate_recognition#Usage Accessed December 2020

[18] Apple contractors 'regularly hear confidential details' on Siri recordings, The Guardian, July 26, 2019.

[19] Foreshadow - Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution. USENIX Security Symposium 2018.

[20] Plundervolt: Software-based Fault Injection Attacks against Intel SGX. Murdock et al. IEEE Symposium on Security and Privacy 2020

[21] CrossTalk: Speculative Data Leaks Across Cores Are Real. Ragab et al. Accepted in the IEEE Symposium on Security and Privacy, 2021.

[22] Why targeted ads are the most brutal owns. Vox, September 25, 2018. https://www.vox.com/the-goods/2018/9/25/17887796/facebook-ad-targeted-algorithm

[23] Google's ad tracking is as creepy as Facebook's. Here's how to disable it. The Guardian, October 21, 2016. https://www.theguardian.com/technology/2016/oct/21/how-to-disable-google-ad-tracking-gmail-youtube-browser-history

[24] Ad Tech Surveillance on the Public Sector Web, Cookiebot Report, version July 14, 2020. https://www.cookiebot.com/media/1136/cookiebot-report-2019-ad-tech-surveillance-2.pdf

[25] Scraping the Web Is a Powerful Tool. Clearview AI Abused It. Wired, January 25, 2020. https://www.wired.com/story/clearview-ai-scraping-web/

[26] Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA. Buzzfeed, February 27, 2020. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement

[27] Secret Users Of Clearview AI's Facial Recognition Dragnet Included A Former Trump Staffer, A Troll, And Conservative Think Tanks. Buzzfeed, March 11, 2020. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-trump-investors-friend-facial-recognition

[28] Researchers Claim Facebook Ads Could Out LGBTQ+ Users. Out, August 30, 2019. https://www.out.com/tech/2019/8/30/researchers-claim-facebook-ads-could-out-lgbtq-users

[29] Resolution on Privacy by Design. 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalem, Israel 27-29 October, 2010. https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacybydesign_en.pdf

[30] Privacy by Design: The 7 Foundational Principles. Ann Cavoukian, Ph.D., Information & Privacy Commissioner of Ontario, Canada. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[31] Qwant. Accessed December 2020. https://www.qwant.com/?l=en

[32] Brave. Accessed December 2020. https://brave.com/

[33] https://www.researchgate.net/publication/301221061_Personalized_Privacy-aware_Image_Classification

[34] Researchers Solve Juniper Backdoor Mystery; Signs Point to NSA, Wired, December 22, 2015. https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/

[35] Is the Intel Management Engine a backdoor? TechRepublic, July 1, 2016. https://www.techrepublic.com/article/is-the-intel-management-engine-a-backdoor/

[36] Encryption: Council adopts resolution on security through encryption and security despite encryption. Council of the EU Press release, December 14, 2020. https://www.consilium.europa.eu/en/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/

[37] Belgian Government Wants To Add Encryption Backdoors To Its Already-Terrible Data Retention Law. Techdirt, October 6, 2021. https://www.techdirt.com/articles/20211003/17223447690/belgian-government-wants-to-add-encryption-backdoors-to-already-terrible-data-retention-law.shtml

[38] Victory! Belgium Scraps Proposed Law to Backdoor End-to-End Encryption. Center for Democracy & Technology, December 22, 2021. https://cdt.org/insights/victory-belgium-scraps-proposed-law-to-backdoor-end-to-end-encryption/

[39] If You Build It, They Will Come: Apple Has Opened the Backdoor to Increased Surveillance and Censorship Around the World, EFF. August 11, 2021. https://www.eff.org/deeplinks/2021/08/if-you-build-it-they-will-come-apple-has-opened-backdoor-increased-surveillance

[40] Keys Under Doormats: mandating insecurity by requiring government access to all data and communications. Abelson et al. MIT CSAIL Technical Report MIT-CSAIL-TR-2015-026. July 6, 2015

[41] End-to-end encryption protects children, says UK information watchdog. The Guardian, January 21, 2022. https://www.theguardian.com/technology/2022/jan/21/end-to-end-encryption-protects-children-says-uk-information-watchdog

[42] Bugs in our Pockets: The Risks of Client-Side Scanning. Abelson et al. CoRR abs/2110.07450. 2021

[43] Apple delays controversial child protection features after privacy outcry. The Verge, September 3, 2021. https://www.theverge.com/2021/9/3/22655644/apple-delays-controversial-child-protection-features-csam-privacy

[43] How overturning Roe v Wade has eroded privacy of personal data. David Cox. BMJ 2022;378:o2075 https://www.bmj.com/content/378/bmj.o2075

[44] How period tracking apps and data privacy fit into a post-Roe v. Wade climate. NPR, June 24, 2022. https://www.npr.org/2022/05/10/1097482967/roe-v-wade-supreme-court-abortion-period-apps

[45] The post-Roe data privacy nightmare is way bigger than period tracking apps. K. Bell. Engadget, June 29, 2022. https://www.engadget.com/data-privacy-period-tracking-apps-130054404.html

[46] Google Says It Will Delete Location Data When Users Visit Abortion Clinics. New York Times, July 1, 2022. https://www.nytimes.com/2022/07/01/technology/google-abortion-location-data.html

[47] A Run a Day Won't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks. K. Dhondt et al. ACM CCS 2022.

[48] Google settles "Location History" lawsuit with 40 states, will pay $392 million. R. Amadeo, Ars Technica. November 14, 2022. https://arstechnica.com/gadgets/2022/11/google-settles-location-history-lawsuit-with-40-states-will-pay-392-million/

[49] There's a Multibillion-Dollar Market for Your Phone's Location Data. J. Keegan and A. Ng, The Markup. September 30, 2021. https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data

[50] Top U.S. Catholic Church official resigns after cellphone data used to track him on Grindr and to gay bars. M. Boorstein et al. New York Times. July 21, 2021. https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/

[51] Sensitive data ruling by Europe's top court could force broad privacy reboot. N. Lomas. TechCrunch. August 2, 2022. https://techcrunch.com/2022/08/02/cjeu-sensitive-data-case/

[52] Facebook Now Cares About How Long You Look At Stuff In Your News Feed. G. Kumparak. TechCrunch. June 12, 2015. https://techcrunch.com/2015/06/12/facebook-now-cares-about-how-long-you-look-at-stuff-in-your-news-feed

[53] Political Campaigns Know Where You've Been. They're Tracking Your Phone. S. Schechner, et al. WSJ. October 10, 2019. https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889

[54] The Radical Scope of Tesla's Data Hoard. M. Harris. IEEE Spectrum. August 3, 2022. https://spectrum.ieee.org/tesla-autopilot-data-scope

[55] Google feels it is 'important' to be able to share Nest Cam recording with police, but never has. B. Schoon. 9to5Google. July 27, 2022. https://9to5google.com/2022/07/27/google-nest-cameras-police/

[56] Digital and Physical Safety: Protecting Confidential Sources. Committee to Protect Journalists. November 22, 2021. https://cpj.org/2021/11/digital-physical-safety-protecting-confidential-sources/

[57] Tesla cars barred for 2 months in Beidaihe, site of China leadership meet. Reuters. June 20, 2022. https://www.reuters.com/business/autos-transportation/chinas-beidaihe-district-bar-tesla-cars-driving-july-local-police-2022-06-20/

[58] Who Actually Owns Tesla's Data? M. Harris. IEEE Spectrum. August 5, 2022. https://spectrum.ieee.org/tesla-autopilot-data-ownership

[59] Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests", KrebOnSecurity, March 29, 2022. https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/

[60] How to encrypt Facebook Messenger chats B. Krasnoff. The Verge. August 17, 2022. https://www.theverge.com/23307995/facebook-messenger-end-to-end-encryption-how-to

[61] Re: Protecting digital rights and freedoms in the Legislation to effectively tackle child abuse. Open letter by European Digital Rights (EDRi) et al. March 17, 2022. https://edri.org/wp-content/uploads/2022/03/Civil-society-open-letter-Protecting-rights-and-freedoms-in-the-upcoming-legislation-to-effectively-tackle-child-abuse.pdf

[62] Proximus Analytics - Big Data - Location Data. Accessed November 22, 2022. https://www.proximus.be/en/id_cl_analytics/companies-and-public-sector/it-services/iot/proximus-analytics.html

[63] GDPR Enforcement Tracker - list of GDPR fines. Accessed November 22, 2022 https://www.enforcementtracker.com/?insights

[64] Post-quantum encryption contender is taken out by single-core PC and 1 hour. D. Goodin. Ars Technica. August 2, 2022. https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/

[65] Securing tomorrow today: Why Google now protects its internal communications from quantum threats. S. Kölbl et al. Google Cloud Blog. November 19, 2022. https://cloud.google.com/blog/products/identity-security/why-google-now-uses-post-quantum-cryptography-for-internal-comms

[66] Post-Quantum Cryptography Standardization | CSRC. NIST. Accessed November 23, 2022. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

[67] GDPR: An impact around the world.. D. Ruiz, Malwarebytes Labs. April 1, 2020. https://www.malwarebytes.com/blog/news/2020/04/gdpr-an-impact-around-the-world

[68] george_orwell_bcn. by fibercool. Taken on July 5, 2007. From https://www.flickr.com/photos/76499396@N00/728743297/ Licensed under CC BY-SA 2.0 https://creativecommons.org/licenses/by-sa/2.0/

Bart Coppens is a part-time assistant professor and a post-doctoral researcher in the electronics department of Ghent University, Ghent, Belgium.

Olivier Zendra is a tenured computer science researcher at Inria, Rennes, France.

This document is part of the HiPEAC Vision available at hipeac.net/vision.

This is release v.3, January 2023. Previous versions were published under the name "Privacy – whether you're aware of it or not, it does matter!"

Cite as: B.Coppens and O. Zendra. Is privacy possible in a digital world? In M. Duranton et al., editors, HiPEAC Vision 2023, pages 130-152, Jan 2023.

DOI: 10.5281/zenodo.7461921

The HiPEAC project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 871174.