Véliz, Carissa. 2019. "The Internet and Privacy," in *Ethics and the Contemporary World*, edited by David Edmonds, 149-159, Abingdon: Routledge.

# The Internet and Privacy

Carissa Véliz
University of Oxford

In 2013, American YouTube music and comedy sensation Chrissy Chambers witnessed her reputation crumble when her ex-boyfriend uploaded seven videos of them having sex to dozens of porn sites. Chambers didn't even know he had filmed her. As the videos spread through the Internet, she was harassed by misogynistic trolls. For months after discovering the videos online, Chambers suffered from night terrors, and body shame so intense that she could not stand to be touched or to look at herself in the mirror. She started drinking, and was diagnosed with post-traumatic stress disorder. In 2017, after four years of legal battle, she reached a settlement with her ex. She received compensation for damages, copyright of the videos, and an apology. It is more than most victims of revenge porn get, but compensation cannot undo psychological damage. And in the Chambers case, her ex's name was not disclosed; as part of the settlement, he kept his privacy.[1]

## What is privacy?

Privacy is the quality of having one's personal information and one's personal 'sensorial space' unaccessed. In other words, you have privacy with respect to another person to the degree that the other person does not have access to your personal information and your personal space—that is, to the degree that they do not know anything personal about you and that they cannot see, touch, or hear you in contexts in which people typically do not want others' attention.

Personal information is the kind of information about ourselves that is common for people in a certain society not to want anyone, other than themselves (and perhaps a very limited number of other people chosen by them), to know about. For example, people typically do not want just anyone to know details about their sex life. Personal information also includes information that the subject is particularly sensitive about and has taken measures to conceal from others. Imagine a person who is shy about her achievements and wishes to keep them secret so as not to become the centre of attention. Similarly, the limits of our sensorial space are set by what people are typically comfortable exposing to others. There are two ways this space can be violated. First, when someone sees, hears, or touches us in a zone in which there are cultural expectations to be free from the eyes, ears, touch, and presence of others (e.g. in the toilet). Access can be obtained through direct or indirect perception (such as cameras and microphones). Second, when we are witnessed engaging in some activity or being

[1] Jenny Kleeman, "The Youtube Star Who Fought Back against Revenge Porn—and Won," *The Guardian*, 18 January 2018.

the subject of some event that typically evokes the desire to have no witnesses or very few chosen witnesses (e.g. being naked).[2]

Chambers' ex-boyfriend violated her privacy because he published content online without her consent that contained sensitive information—that she had had sexual intercourse with a man. This information was particularly problematic because in online communities she described herself as a lesbian. The violation of her privacy was compounded by the use of images—except for exhibitionists, most people do not want to be seen naked nor witnessed when having an intimate experience with another person.

But why should we value privacy?

Well, because having our personal information accessed and our sensorial space invaded makes us vulnerable. Privacy protects us from both individual and collective harms.

**Individual harms**

One set of harms that privacy protects us from is illustrated by revenge porn—the non-consensual sharing of nude or sexual images—and related harms such as blackmail. Others' attention and judgment can cause people to feel self-conscious at best, and humiliated or shunned at worst.

Revenge porn is not uncommon. According to a survey of nearly 4,300 people, one in five Australians has been a victim of image-based abuse. In some cases, sensitive images get shared and exposed; in other cases, the threat of exposure is used to coerce, extort, or harass the victim.[3] In England and Wales, 1,160 cases were reported to the police in the first nine months after the legislation on revenge porn was passed in 2015. Some victims were as young as 11 years old.[4]

Other individual harms include identity theft and fraud. A woman who got hold of Ramona María Timaru's personal details used them to impersonate her and take out loans in banks across Spain that were never paid back. It is surprisingly difficult to prove you did not commit a crime when someone is committing them in your name. Timaru has been detained multiple times, and she has spent years and a substantial amount of money defending herself in many trials in different parts of Spain. When the newspaper *El País* interviewed her, she said that her life 'was being ruined,' and that she was taking tranquilisers to fight anxiety.[5]

Some other individual harms are more difficult to notice, but can be just as damaging. One is discrimination. Data brokers are companies that strive to collect all the data they can on Internet users. Information can include census and address records, driving

[2] Carissa Véliz, "On Privacy" (University of Oxford, 2017).
[3] Nicola Henry, Anastasia Powell, and Asher Flynn, "Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse," (Melbourne: RMIT University, 2017).
[4] Peter Sherlock, "Revenge Pornography Victims as Young as 11, Investigation Finds," *BBC*, 27 April 2016.
[5] José Antonio Hernández, "Me Han Robado La Identidad Y Estoy a Base De Lexatín; Yo No Soy Una Delincuente," *El País*, 24 August 2016.

records, web-browsing history, social media data, criminal records, academic records, credit records, medical records, and more. They then sell these files to banks, would-be employers, insurance companies, and governments, among others.

Imagine two candidates are equally qualified for a particular job, but the data broker's file on one of them shows that he suffers from health issues. The company decides to hire the healthy candidate and tells the other one that there was someone more qualified for the job. In theory, discrimination is illegal. In practice, it is very hard to prove; companies can always come up with untruthful explanations for their decisions, and victims may not even realise they have been discriminated against. Discrimination may take several forms: if your genetic information is not private, an insurance company that suspects you to have bad genes can charge more expensive premiums for something over which you have no control and for which you cannot be blamed.

**Collective harms**

Privacy damages can also be collective. In the 2018 Cambridge Analytica scandal, it was revealed that personal data from 87 million Facebook accounts had helped build psychological profiles of Internet users who were then sent personalised political propaganda. Cambridge Analytica worked on both the 2016 US election and the EU referendum campaign in Britain that same year. During the referendum, the firm was on the 'leave' side; voters who were leaning towards voting 'leave' got information that reinforced their views, including false news regarding immigration, while voters who were thinking of voting 'remain' might have been sent information that discouraged them from going to the ballot box. Propaganda is not new, but in the past it was something public—everybody could see what each party was advertising. What is particularly unhealthy about personalised propaganda is that it contributes to polarisation through showing each person different and potentially information, and it takes advantage of people's personality traits to be more effective in influencing them. In the past, propaganda may have been just as misleading, but at least we all had access to it. Personalised propaganda causes individuals to be blind to what others' are seeing. It fractures the public sphere into atomic individual spheres.

One lesson of the Cambridge Analytica case is the collective nature of privacy. Privacy is not only collective because of the consequences of its loss—even if 'only' 87 million Facebook users lost their privacy, all of the citizens of the manipulated democracies were indirectly harmed. Privacy is also collective in another way: when you expose information about yourself, you inevitably expose others as well.

Only 270,000 Facebook users actually consented to Cambridge Analytica collecting their data. The other 87 million people were friends of the consenting users whose data was harvested without their knowledge or consent. We are responsible for each other's privacy because we are connected in ways that make us vulnerable to each other. Think of all the contacts you have on your mobile phone. If you give a company access to that phone, you give it access to your contacts too. If you divulge genetic information, you expose your parents, siblings, and children. If you reveal your location data, you inform on people with whom you live and work. If you disclose your habits and psychological make-up, you expose people who resemble you.

Collective harms facilitated by privacy losses can be dramatic. The Nazis were more effective in finding Jews where there were better civil registers. It is no coincidence that the Nazis were great innovators in techniques of registration and identification of individuals. It is worth noting – given the new power of technology companies –that it was a technology company, IBM, who assisted them in these objectives through the development of punch cards.[6]

These examples may come from what might seem the distant past. But as I write this, the Chinese government is implementing a system of 'social credit' through which people are given a grade that represents their reputation. It is calculated on the basis of all the data that is held on them. A poor grade may limit their access to opportunities. In February 2017, the Supreme People's Court announced that 6.15 million people had been banned from taking flights in the last four years for having committed 'social misdeeds.' Another 1.65 million people on the blacklist are banned from taking trains.[7] The Chinese government is creating a system of control over its citizens in which as many individual actions are recorded as possible; those who deviate from established norms are punished with social exclusion or worse. The government knows so much about its citizens that dissidence can be squashed before it can express itself in an organised fashion. And if it does appear, those who engage in it can be easily targeted for punishment.

For those of us lucky enough to live in reasonably democratic societies, the mere existence of data on us is still a risk. Democratic countries have not always been democracies, and may cease to be so in the future. Data is like water—it rarely stays still and isolated. It tends to combine and flow. There is no telling in whose hands it may end up.

**Data hygiene**

Hoarding personal data is a risky practice. This information is coveted by many agents—from personal enemies, jealous exes, and bad neighbours, to insurance companies, business competitors, data brokers, banks, and governments. Information is hard to keep safe in the digital age. Attackers will always have an advantage over defenders. An attacker can choose the time and method of attack, while defenders have to protect themselves from any type of attack at all times. A sufficiently skilled, motivated, and well-funded cyber-attacker has a high probability of success. And that is if the defender is doing everything it can to protect data. But netizens cannot trust that governments and companies will be careful enough with their data. Even if they do not sell data—which, in this data economy should not be taken for granted—governments and businesses can be sloppy about keeping data safe. In 2015, the American government was hacked and sensitive information on 21.5 million people who had undergone background checks for security clearances was stolen.[8]

---

[6] Edwin Black, *Ibm and the Holocaust* (Washington, DC: Dialog Press, 2012).
[7] Rachel Botsman, "Big Data Meets Big Brother as China Moves to Rate Its Citizens," *Wired*2017
[8] Patricia Zengerle and Megan Cassella, "Millions More Americans Hit by Government Personnel Data Hack," *Reuters*, 9 July 2015.

Since data is vulnerable, data subjects and anyone who stores data are also vulnerable. This is why Security expert Bruce Shneier calls personal data a 'toxic asset.' [9] It is like keeping a bomb in the shed that could explode at any moment.

Given the destructive potential of personal data, one strategy is to lose as little privacy as possible. This advice, however, is not very practical in the current digital environment. To be fully functional members of society, most of us feel compelled to use services like Facebook and Twitter that force us to give up some privacy. These platforms have become the new public square; suggesting we stay away from them may be too much to ask. As democracies, we also do not want to discourage citizens from participating in new forms of public engagement. In any case, companies like Facebook track netizens online even if they do not have a Facebook account; opting out is not always an option.

Fortunately, 'abstinence' is not the only or even the safest way to protect privacy online. Useful advice includes being conservative in all privacy settings, covering your cameras with tape or a sticker, staying away from online quizzes that ask personal questions, using ad blockers, turning off your phone's Wi-Fi and Bluetooth when you leave home, choosing services that are better at protecting privacy (e.g. DuckDuckGo instead of Google, ProtonMail instead of Gmail, etc.), and using obfuscation. Obfuscation means confusing online trackers, losing them with noise.[10] In some cases, like government webpages, the law requires you to reveal your identity. But online companies do not have a claim on your personal data. If they force you to give up personal data in exchange for services, you are entitled to give them misleading information about your birth date (as long as you are not a minor trying to access a service for adults, or an adult pretending to be a minor), gender, location, or preferences. There are a few tools that have been designed to facilitate obfuscation. TrackMeNot, for example, issues randomised search-queries to popular search engines to hide your actual searches and interests.

Most important of all is to periodically delete old data that is no longer necessary. Privacy expert Max Schrems deletes his tweets after they have been published for two months. You might find that deleting personal data is hard. The temptation is to hold on to it as a way of holding on to your history, your identity. But keeping personal data online is dangerous. Getting rid of it is a way of making sure you will not get stuck in the past or in a mistake—a drunken night, a bad relationship, an unreflective comment, or an opinion you no longer hold or in any case don't want in the public domain.

That is the motivation behind the European right to be forgotten. In May 2014, the European Court of Justice ruled against Google in *Costeja*, a case brought by a Spanish man, Mario Costeja González, who requested the removal of a link to a digitised 1998 article in a newspaper about an auction for his foreclosed home, for a debt that he had subsequently paid.[11] If he had already paid his debts, he successfully argued, it was unfair for his reputation to continue to be tarnished. If our mistakes

[9] Bruce Schneier, "Data Is a Toxic Asset, So Why Not Throw It Out?," *CNN* 2016.
[10] Julia Powles, "Obfuscation: How Leaving a Trail of Confusion Can Beat Online Surveillance," *The Guardian*, 24 October 2015.
[11] Bygrave, Lee Andrew. 'A Right to Be Forgotten?,' *Communications of the ACM,* 58:1, 35-37, 2015.

become the only thing we are known for (as people usually read only what comes up first on a search engine), we will never be allowed to move past them.

Under the European General Data Protection Regulation (GDPR), data subjects now have the right to ask institutions and businesses to erase their data, stop sharing their data, and have third parties halt processing of the data. Although the law only applies to European citizens, many companies, including Facebook, have vowed to extend the same rights to all its users. The success of the legislation will partly depend on users demanding our rights. No good will come from the right to be forgotten unless netizens actually ask for their data to be deleted.

## Conclusion

In 2010, Facebook founder Mark Zuckerberg suggested that privacy was no longer 'a social norm,' that we had 'evolved' beyond it. It is unclear whether he really meant this. He bought the four houses surrounding his for privacy reasons, which rather casts doubt on his sincerity. What is clear is that he was wrong. Privacy is as important and relevant as ever - in fact, in the digital age, more relevant than ever. When we fail to protect privacy, individuals and societies get harmed.

These harms suggest that privacy is not only a right on account of the interests we have in protecting our personal information and sensory space; it is also an obligation. We do not only put ourselves at risk when we are careless with our privacy. We also jeopardise our family, friends, flatmates, colleagues, fellow citizens, and people with whom we share habits and personality traits. A culture of exposure creates a hostile environment for anyone identified as an outlier. Protecting our privacy is thus not only an act of self-care, but it is also necessary to protect others' privacy.

The need for privacy is as important as the need for companionship and community. In fact, these goods are complementary. Privacy is necessary for individuals and communities to thrive. We are not creatures who thrive in fishbowls.

## References

Black, Edwin. *Ibm and the Holocaust*. Washington, DC: Dialog Press, 2012.

Botsman, Rachel. "Big Data Meets Big Brother as China Moves to Rate Its Citizens." *Wired*, 2017.

Bygrave, Lee Andrew. 'A Right to Be Forgotten?,' *Communications of the ACM,* 58:1, 35-37, 2015.

Henry, Nicola, Anastasia Powell, and Asher Flynn. "Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse." Melbourne: RMIT University, 2017.

Hernández, José Antonio. "Me Han Robado La Identidad Y Estoy a Base De Lexatín; Yo No Soy Una Delincuente." *El País*, 24 August 2016 2016.

Kleeman, Jenny. "The Youtube Star Who Fought Back against Revenge Porn—and Won." *The Guardian*, 18 January 2018.

Powles, Julia. "Obfuscation: How Leaving a Trail of Confusion Can Beat Online Surveillance." *The Guardian*, 24 October 2015 2015.

Schneier, Bruce. "Data Is a Toxic Asset, So Why Not Throw It Out?" *CNN*, 2016.

Sherlock, Peter. "Revenge Pornography Victims as Young as 11, Investigation Finds." *BBC*, 27 April 2016.
Véliz, Carissa. "On Privacy." University of Oxford, 2017.
Zengerle, Patricia, and Megan Cassella. "Millions More Americans Hit by Government Personnel Data Hack." *Reuters*, 9 July 2015.