the ethi{CS} project

The Ethics of Data Privacy

By: Kiran Bhardwaj

Users and creators of technical tools face competing data privacy priorities between **convenience** and **security**. We want the added convenience of being able to have easy access to our private information and to share that access with those we choose. Yet there are those we don't want to have our private information: actors with malicious intents, conflicting interests, or those who simply don't need it. So we should ask ourselves: how should we resolve this tension?

What is privacy?

One of my favorite philosophers (Helen Nissenbaum!) suggests that we can conceive of what we want from privacy not as secrecy, per se, but in terms of two sets of considerations:

1. *Appropriateness*: *what kind of information is contextually appropriate (and inappropriate)?* While I might accept that my preferred social media site will have access to some personal information so I can share with my friends, I wouldn't consider it appropriate for my bank to have that information (and vice versa: I wouldn't want my social media site to have access to my financial records). A disclosure of the wrong type information to the wrong kind of entity or individual would be a breach of privacy.
2. *Flow: what are our expectations about how information will be transferred between third parties?* We expect the information that we post on social media to only be accessible to those who we're friends with, and not released to employers or the world at large. We expect financial institutions to keep our financial information secure, without releasing it to others. A flow of information contrary to our expectations would be a breach of privacy.

How are privacy norms set?

We each have different comfort levels about who has our private information. My mother, for example, is deeply uncomfortable with anyone besides immediate family and close friends having her birthdate, and gives false dates to Facebook and other online companies. Others are comfortable if the world at large has information that can be sensitive (e.g., salary, health conditions)—in fact, they may argue that revealing such information might allow us to undo pay disparities or reduce stigmas. One conclusion we could draw is that each person should share what they want to whom they want. Perhaps institutions should offer us fine-grained control for who has access to my information.

However, there are reasons to *not* allow full discretion to individuals: we sometimes want to keep information private although others have a right to it (e.g., the spouse you're divorcing is allowed access to pertinent financial information while the terms of divorce are being settled, whether you want to share or not). In other cases, we might think that we should not be allowed to share information that we might later regret disclosing (that we should be protected from ourselves). So we do want some regulations to ensure that the ways in which private information is released (or not) abide by standards beyond 'what I want'.

Perhaps a better solution is to appeal some underlying ethical *reason* (e.g., to prevent harm, promote personal autonomy, or to preserve more equality) for how we should demarcate our rights to privacy. Doing so might allow us to make claims about privacy for principled reasons, which avoids the worry about personal preferences being too arbitrary.

Who bears the burden to protect individuals' private data?

Finally, who is responsible for protecting our privacy—governments, companies, individuals? Each may have a role to play, but there are disagreements about their roles and ethical obligations.

Governments might have an obligation to protect users because they have the power to create regulations and can use their oversight to ensure that companies abide by these practices. However, we might think that a given government will not protect privacy enough or in the right way, or their regulations may not 'have teeth' or be enforced at all. Companies might have an obligation to protect users' privacy because they are best-placed to design their products and services to meet a moral obligation to protect and enhance individuals' privacy. Of course, if companies have a business model where their interests are contrary to the interests of users, they may not take these measures.

Do we have an obligation to protect our own privacy? We might say so, especially in the face of cases in which governments and companies fail to protect us. However, we have practical limitations: even if I'm upset at the government's or a tech company's privacy practices, I (as an individual) cannot get them to stop or change their practices. At best, I can go for lower-hanging fruit: being mindful of what I share, using secure passwords, and the like.

Have our options run out? Some philosophers (such as Anita Allen) argue that even though we don't have enough power as individuals, we can (and ought to) engage in collective action in order to get governments and companies to modify their practices. So, perhaps I have to do more than take action on my own: I need to coordinate with others so that we, together, can work to protect privacy.

Further Resources:

- Stanford Encyclopedia of Philosophy article on "Privacy and Information Technology"
- Anita Allen, "Protecting One's Own Privacy in a Big Data Economy"
- Helen Nissenbaum, "Privacy as Contextual Integrity", *Washington Law Review* (2004) particularly pp. 120-125.