Tech Ethics Animated – Privacy

Transcript

In 2012, a retail company looked to answer the question, “If we wanted to figure out if a customer is pregnant, even if she didn’t want us to know, can you do that?” The answer was yes. The company could now predict if a customer was pregnant based on their past purchases. This opened the door for targeted advertising as the company could now send personalized ads to a targeted audience of one. Advertisements arrived at the pregnant woman's house, revealing the secret of her pregnancy status to others in the household. While this is an old case, this is still a current problem where companies violate privacy by aggregating data to infer new information about users.

The company was legitimately gathering and storing customer data. However, this particular use of the data was a violation of privacy. So what makes up an act that “violates my privacy”? To answer that question we must define privacy. Scholars’ and regulators' definition of privacy varies. How you define privacy impacts how it is protected and an individual’s rights to privacy in a given situation.

Traditionally, two definitions of privacy have been used. First, the restricted access view of privacy defines privacy as where access is restricted or what is hidden from the public eye. When someone shops online, uses apps, and even goes outside, this view suggests that the individual no longer has expectations of privacy since the information is no longer restricted. This version of privacy does not account for our regular expectations of privacy around information shared with friends, doctors, teachers, corporations, online interactions, and more.

Second, the control view of privacy defines privacy as the degree of control someone has over their person and information. With more control comes more privacy. While users seek more control over the type of data, who has access to that data, and how that data will be used, companies obtain more control since they are the ones to set the policies within their notices. In the United States, the FTC’s Fair Information Practice Principles puts “privacy as control” into practice. It is now required by the FTC for companies to provide adequate notification and consent for the use of their online services. Consumers hold the control as they can read the notice and have the option to continue to engage with the company and its services. However, companies tend to make convoluted and ambiguous notices that do not explain the companies' data collection practices. Notices are rarely read, and if read, not understood by the consumer. Consumers more often assume that their privacy expectations are met when notices are present. Oftentimes, users even project their privacy expectations onto the

notice. When asked, they will make assumptions based on their own views of what is contained in the notice without having any idea of the actual contents of the notice.

Both these views would support the idea that the retail store did nothing wrong. As soon as information is made public, these theories would suggest that you no longer have any privacy expectations. This is not the case as we regularly have expectations for privacy in public or after we share our information with someone. For instance, the original story of peeping Tom reinforces the idea that even when out in public, privacy can be violated by someone else.

The story of “peeping Tom” was focused on the concept of privacy in the public eye. As the folktale has it, Lady Godiva begged her husband, the local Earle, for months to lift the burdensome taxes on his people. The Earle finally said he would lift the taxes only if she rode through the town naked on horseback. In order to achieve this goal, all the people in town agreed to avert their eyes and face in the other direction as she rode through town. The only person that turned and looked at her was the town's tailor, Tom. Peeping Tom violated the privacy expectations of Lady Godiva while in public. There were norms on how to behave, everyone was to turn their back, and Tom broke those norms. Even when out in public, Lady Godiva had privacy until Tom turned around. This story suggests that we have long had privacy even when in public.

In other words, there is no place where, as Helen Nissenbaum says, anything goes. There are always terms of use or norms governing how data should be gathered, used, shared, and aggregated. Whether you are sharing information with a doctor, teacher, or even a retail store, there will still be norms. Nissenbaum's theory is based on the idea that there is an appropriate flow of information. Her theory of privacy as contextual integrity suggests that privacy is the respect for the norms around the data use and who has access to the data within a particular community. For instance, within the medical community, there is a specific set of norms. She focuses on whether the data being gathered and used, those who have access to the data, and the transmission principle is appropriate for the given context. As long as appropriate, privacy expectations are met. Any diversion, however, would be a violation of privacy. Under her theory, the retail company was not abiding by appropriate norms as the company tried to get new data, guessing at intimate health information and telling someone else about the new data.

CREDITS

Animation Team

Michael Simon (Lead)

Josiah Broughton

Script

Brooke Anquillare

Faculty Advisor

Carolina Villegas-Galaviz, Ph.D.

Associated Readings
Martin, K. (2022). Privacy, Data, and Shared Responsibility. In *Ethics of Data and Analytics: Concepts and Cases*. Taylor & Francis: USA, 93-96.
Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, 140(4), 32-48.
Martin, K. (2016). Understanding Privacy Online: Development of a Social Contract Approach to Privacy. *Journal of Business Ethics*, 137(3), 551-569.
Duhigg, C. (2012). How Companies Learn Your Secrets. *The New York Times*.

Technology Ethics Center

UNIVERSITY OF NOTRE DAME