# Avoid a privacy nightmare with 'Lean Privacy Review'

November 21 2021, by Daniel Tkacik


A privacy storyboard illustrating data practices during the scenario of using a loyalty card in a retail store. Credit: CyLab

When Google launched its own attempt at a social network—Google Buzz—back in 2010, the company initially suffered a PR nightmare. "WARNING: Google Buzz Has A Huge Privacy Flaw," read Business Insider. It turned out, Google was generating user connections by collecting contact info from users' Gmail accounts. In other words,

anyone on the social network could see who anyone else's personal contacts were.

To try to avoid privacy nightmares like that one, companies sometimes perform privacy reviews on new applications or services to try to catch any potential privacy issues before they're released. These reviews typically involve privacy experts and lawyers and tend to cost quite a bit of money and time, making them not very feasible for many companies. They also rarely involve actual user feedback.

But a recent study by Carnegie Mellon University CyLab researchers proposes a new kind of privacy review—one that is cheaper and makes it easy to hear direct user feedback early in the development process. The study, "Lean Privacy Review: Collecting Users' Privacy Concerns of Data Practices at a Low Cost," was published in the current issue of *ACM Transactions on Computer-Human Interaction*.

"Lean Privacy Review can help reveal privacy concerns actual people can have at a tiny fraction of the cost and wait-time for a formal review," says Haojian Jin, a Ph.D. student in the Human-Computer Interaction Institute (HCII) and the study's lead author.

The authors say that a Lean Privacy Review—or LPR for short—isn't meant to replace the formal privacy review—privacy experts and lawyers are still necessary—but rather to supplement the formal review to make the whole process easier and smoother. They say that LPR is especially useful in the very early stages of design.

"If you can find these problems much earlier on, and cheaper, it's actually good for everybody," says CyLab's Jason Hong, a professor in the HCII and a co-author of the study. "The speed and low cost of LPR increases its flexibility and allows it to be used more often and throughout the entire design process rather than just a one-time formal

privacy review."

LPR begins when a practitioner wants to understand users' privacy concerns of using a certain type of data for a specific purpose. They'll create a privacy storyboard using the LPR website to communicate one or any of the four main actions performed on that data: data collection, sharing, processing, and usage. Using the storyboard, the website will then create a survey for users, in which they describe the data action, and then ask how they feel about the action, and why in plain English. The practitioner may distribute the survey through any number of survey channels, e.g. crowd workers on Amazon Mechanical Turk or Google Marketing Platform.

After the survey has been conducted, a web interface aggregates all of the privacy concerns identified by users into a series of graphics.

"Through these visualizations, practitioners can have both a quantitative and qualitative view of potential privacy concerns, namely, how severely the concerns are and what the concerns are," says Jin.

The researchers evaluated LPR using 12 real-world data practice scenarios—including the Google Buzz scenario—with 240 crowd users and 24 data practitioners. They found that it only takes ~ 14 participants to find the vast majority of the privacy concerns and costs less than four hours of total crowd work for a given scenario. That's equivalent to about $80.

"Our results show that LPR is inexpensive, fast, consistent, and can provide high-quality privacy review results," the authors write in the study.

It's hard to know for sure what kind of privacy review, if any, Google had performed before launching Google Buzz (the company did address

the issues relatively quickly after the public uproar), but it's possible they could have dodged their privacy nightmare if they'd had LPR.

For those interested, LPR has a website where one can explore the method and create storyboards.

**More information:** Haojian Jin et al, Lean Privacy Review: Collecting Users' Privacy Concerns of Data Practices at a Low Cost, *ACM Transactions on Computer-Human Interaction* (2021). DOI: 10.1145/3463910

Provided by Carnegie Mellon University