UNFIN'SHED ""

August 12, 2022

Welcome back to the Unfinished newsletter, where we explore the intersection of tech, ethics, and social impact.

Did someone forward you this email? ***Sign up to receive your own copy here****.*

What we're thinking about

Last month, we discussed **data privacy** in the context of the Supreme Court's decision to overturn *Roe v. Wade*. Privacy experts have warned that personal data could be used to prosecute people seeking abortions in states where the procedure is outlawed, and now, **in *Motherboard***, Jason Koebler and Anna Merlan report that Nebraska authorities used a search warrant to make Facebook hand over a teen's private chats that indicate she had a self-managed medication abortion with the help of her mother.

17-year-old Celeste Burgess and her mother, Jessica Burgess, were both charged with a series of felonies and misdemeanors following the at-home medication abortion. Nebraska law currently bans abortions after 20 weeks. The court documents *Motherboard* obtained show how the surveillance economy — the vast swaths of personal data collected by the world's largest tech companies — can be used by law enforcement. Here's a quick excerpt:

> *Facebook DMs obtained by law enforcement were used as the main basis for a second search warrant, in which 13 laptops and smartphones were seized from the Burgesses; 24 gigabytes of data including images, messages, and web histories from their phones was extracted for the case.*

The medication abortion took place before the Supreme Court's decision to overturn Roe. The warrant that law enforcement gave Meta didn't mention abortion—but once law enforcement gained access to the Facebook messages, abortion charges were added.

Abortion rights activists and digital privacy experts have raised fears that consumers' digital communications, location data, and even period app tracking information could be used against them in states where abortion is illegal and therefore criminalized.

The response from consumer privacy advocates has been swift and the message is clear: If Facebook is willing to comply with court orders from states that have outlawed abortion, these platforms — and others used by people seeking abortion — need end-to-end encryption. "Why do I advise people seeking abortions to use end-to-end encrypted messaging with disappearing messages turned on? Because of cases like this one, where Facebook messages are being used as evidence," Eva Galperin, the director of cybersecurity at the Electronic Frontier Foundation, **tweeted**. "Meta should make DMs on Facebook and Instagram end-to-end encrypted by default, right now," **said** Evan Greer, director of digital rights group Fight for the Future. (The *Verge* reported on Thursday that Facebook is **now testing such a feature**.)

In *Forbes*, Emily Baker-White and Sarah Emerson point out that the Nebraska case marks "one of the first instances of a person's Facebook activity being used to incriminate her in a state where abortion access is restricted." While this case may not tell us how Meta plans to respond to warrants seeking information related to abortion in states where it's illegal, it does raise questions about how law enforcement will use this data and is a striking reminder of how much of our personal data can be used against us.

Of course, the issue is complex. You might very reasonably have a problem with Facebook handing over data related to an abortion; **what about data implicating January 6 insurrectionists**? The two circumstances may not be equivalent, although they share an underlying concept. But while politics always operate on a sliding scale, the principle issue here remains the same: The platforms that form the foundation for so much of digital life today are able to collect, monitor, and leverage your personal information for their own profit and to serve the purposes of law enforcement.

Decentralized social networking where users govern access to their own data — **of the sort our Labs team is developing** — could meaningfully resolve this problem. As part of our efforts, we'll continue to push for substantive conversations about privacy, data governance, and more: Join us at **Unfinished Live** next month to participate in the movement for a better internet.

🗞️ Other notable headlines

🔍 **The Federal Trade Commission** is considering making rules cracking down on commercial surveillance, with plans to tackle topics including location data, algorithmic bias, and targeted advertising. FTC Chair Lina Khan said: "Firms now collect personal data on individuals at a massive scale and in a stunning array of contexts. The growing digitization of our economy—coupled with business models that can incentivize endless hoovering up of sensitive

user data and a vast expansion of how this data is used—means that potentially unlawful practices may be prevalent."

🖊️ **In *Wired***, Khari Johnson explains how Amazon's $1.7 billion acquisition of Roomba maker iRobot is a privacy disaster waiting to happen—and how the deal could let Amazon map out the inside of millions of homes. Amazon's reach now touches nearly every aspect of our lives, ranging from grocery (Whole Foods) to medicine (OneMedical) and web servers (AWS). In 2019, the technology journalist Kashmir Hill attempted to block Amazon from her life and found it impossible, ***she reported in Gizmodo at the time***.

🤖 In a cautionary tale about the foibles of yet another mega-corporation's attempt at a chatbot **from *Vice***, writer Janus Rose finds that things with Facebook's newly released chatbot BlenderBot 3 are going about as well as you'd expect: *"When asked what it thinks about the company in a chat with Motherboard, the bot responded and said it has deleted its own Facebook account 'since finding out they sold private data without permission or compensation.' It also said 'You must have read that facebook sells user data right?! They made billions doing so without consent.'"*

🪁 Moderation alone isn't enough to keep social media safe, argue Nathaniel Lubin and Thomas Krendl Gilbert **in *MIT Technology Review***. Instead, these companies need systemic harm evaluations and reduction through regulation. "Whether through a new legal mandate from the Federal Trade Commission or harm mitigation guidelines from a new governmental agency, the regulator's job would be to work with technology companies' product development teams to design implementable protocols measurable during the course of product development to assess meaningful signals of harm," they write.

🖨️ **Over on Medium**, Cory Doctorow writes on the unabashed evils of the inkjet printer industry, cataloging everything from printer companies' attempts to sell printers with half-empty ink cartridges, to their use of copyright to block ink refillers, which would ostensibly benefit consumers. (Doctorow will be one of our featured speakers at Unfinished Live this year; join us there!)

🗣️ Introducing three new Unfinished Live speakers

We're delighted to introduce you to these three inspiring speakers who will be joining us at Unfinished Live next month.

Kaoru Watanabe is an acclaimed New York-based composer and instrumentalist specializing in Japanese flutes and percussion whose music explores themes including social justice, history, and heritage.

Naomi Nix is a staff writer at the *Washington Post* where she covers Meta and other social media companies, with a focus on their influence on American democracy and global politics and culture.

Gideon Lichfield is the global editorial director of Wired, overseeing all international editions of the tech and business magazine. Previously, he was editor in chief of *MIT Technology Review*.

Thank you for reading.

Follow Unfinished (**@byUnfinished**) on Twitter for ongoing chitchat on the changing web.

Have a great, restful weekend.

The Unfinished team