UNFINISHED

July 8, 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 week, **we discussed data privacy** in the context of the Supreme Court's decision to overturn Roe v. Wade. This week, our attention is turned to another national crisis and its unfortunate intersection with digital life.

On July 4, seven people were killed in a mass shooting at an Independence Day parade in Highland Park, Illinois. Almost immediately, the shooter's online presence was mined and exploited by bad actors — a familiar aftershock of this kind of public attack that highlights a profoundly complex content moderation issue.

Tech companies "are still not fast enough to prevent a dangerous knock-on effect of the violence," Bloomberg reporters Davey Alba and Cecilia D'Anastasio **wrote in a story** on Wednesday. "Social media users themselves swiftly find, circulate and discuss the shooter's posts, in some cases creating a glorification and amplification of murder that could inspire other shootings and that the technology industry—for all its engineering might—remains ill-equipped to contain."

They continue:

> *Some of this propaganda is intended to sow chaos and social conflict that, some extremists hope, will create conditions for a new society aligned with their views—a philosophy known as "accelerationism." Other times, posts apparently valorizing these individuals are not explicitly politically motivated; irreverent internet users on forums such as 4chan use imagery from these tragedies to make edgy jokes.*

> *[The July 4th shooter's] motivations are less traceable to known extremist groups. In fringe communities such as 4chan and Gab, users exchanged conspiratorial theories, picking apart images of him wearing a Trump flag around his shoulders and a rose tattoo as clues for his ideological affiliation. The online obsession around shooters plays into what many of them envision as their legacy.*

In other words, these horrific acts of physical violence also cast a long digital shadow. Platforms like Facebook and YouTube thrive on users creating and sharing content, as the resulting data can be bundled up and leveraged to drive engagement and target advertisements. Remember that the platform that allows a shooter's manifesto to spread in Facebook Groups is the same platform that allows a Facebook Page to serve you an ad for orange juice. In this sense, it may not be enough to simply remove offending bits of content as they pop up. The digital economy underpinning this content — the system itself — must also be reset.

If you're interested in mulling over this challenge, a brief 2021 piece from the tech journalist Will Oremus, "**How to Start Fixing Social Media**," is a good place to start. Although he was addressing a very different context — the role of social media in the January 6 insurrection — many of the ideas explored in the story have direct relevance to this situation.

"One school of thought holds that the big social media companies are capable of doing better, even if they must be pushed, regulated, and cajoled into it," he writes. "Another group of tech critics regards today's social media environment as fundamentally broken, and focuses accordingly on rethinking the entire project."

This may be one of the most consequential challenges of our time. We're working to tackle it through **Project Liberty**, a multidisciplinary effort to build a new civic architecture for our digital future. (For more on that, we invite you to **watch this recent panel discussion from Polkadot Decoded**.) After all, as Buckminster Fuller said, "To change something, build a new model that makes the existing model obsolete."

💬 *Psst… on that note… If you want to be part of the movement to build these new solutions, join us **at Unfinished Live this year**.*

Other notable headlines

🇨🇳 Speaking of data disasters, **Karen Hao and Rachel Liang report in the *Wall Street Journal*** that a massive police database containing personal information on nearly 1 billion people was ransacked by an anonymous party. It contains names, birthdays, addresses, government IDs and photos, phone numbers and more — like, "a label for 'people who should be closely monitored,' a designation often used in China's government surveillance systems to denote people seen as posing a threat to social order." A good reminder that your personal data is only as secure as the vault storing it.

🦠 Many Covid-tracking apps are now pivoting to a variety of money-making schemes, **Matt Reynolds and Morgan Meaker report in *Wired***. It's a true lesson in a kind of digital consent most of us probably don't think too much about: When you sign up for an app today, should you have to worry about what it's going to look like two years from now? "In Berlin, a contact-tracing app called Luca is reinventing itself as a payment system, while in northern Italy an app set up to track coronavirus cases now warns citizens about natural disasters," Reynolds and Meaker write. "With the most urgent phase of the pandemic now over, developers are looking for ways to squeeze more value out of the users who have downloaded their apps."

💰 **Cheyenne Ligon reports in *CoinDesk*** that "U.S. officials who are personally invested in cryptocurrencies are now disqualified from working on crypto-related policy and regulation that could affect the value of their assets." Crypto lobbying, however, which has **ballooned to a multimillion-dollar industry of late**, will no doubt continue apace.

🙋Listen to our latest Unfinished Conversation

On Thursday, we convened a panel of experts to talk about data privacy in the post-Roe world. We'd like to share two core insights from our panelists, lightly edited for clarity:

🗣️ **Jackie Singh, Director of Technology and Operations at the Surveillance Technology Oversight Project, shared her concerns about how digital services are able to cross-pollinate:**

> *The real problem with data privacy is that [services are] collecting so much information, and we're allowing so many different organizations to warehouse this information in an attempt to profile us. And the fact is, we don't have access to any of these profiles. We don't have these dossiers. I don't know what my period apps have on me—what other conclusions have they drawn about me based on my other usage of apps on my phone? What else have they been able to glean, not just from me putting in my data, but from my interactions with other devices and other other applications?*
>
> *People don't really understand that they're all sharing data, and that this is an entire surveillance capitalism ecosystem.*

🗣️ **Shoshana Wodinsky, Data Reporter at Gizmodo, discussed how real-world clinics intersect with tracking services:**

> *Companies collect data about you from all of these different touch points. They might be collecting data from your mobile phone by using a beacon at the door when you walk inside. They might have a cookie that's on*

their web page when you click a link that you think is an abortion clinic, but it's actually [a crisis pregnancy center]. They might have some sort of call-tracking software that is perfectly legal. But you, the average person, has no idea it exists when you're talking to them on the phone.

The thing is, the companies that are controlling these cookies or the software or whatever the heck — it's not going to be the clinic. The clinic is outsourcing that to third parties. So, even if the clinic might [not want to give up data] … there's literally thousands of third parties that these organizations could be working with. They likely know more about you than the clinic does.

Listen to the full conversation here. And join us on Twitter Spaces in two weeks for our next session — details to come in next week's newsletter.

💡 Join our next Unfinished Salon

As we mentioned above, this September, we're taking over The Shed in NYC for **Unfinished Live**, our annual festival exploring the collision of technology, art, ideas, and impact. The four-day program is really shaping up, and we hope you'll follow along this summer as we announce new speakers, sessions, and events.

There is much to discuss about the future that's rapidly taking shape all around us, which is why we're hosting Twitter Spaces and virtual salons to keep the conversation going year round. We'd love to see you at our next salon, taking place from 2-3pm ET on Wednesday, July 13, where we'll explore a question that's at the very heart of our work: **How can we reimagine digital tech to build a thriving multiracial democracy?**

We'll be joined by Claudia Peña, Executive Director of **For Freedoms**, Prakash Janakiraman, Co-Founder and Chief Architect of **Nextdoor**, Pia Mancini, Co-Founder and CEO of **Open Collective**, and Deepti Doshi, Co-Director of **New_ Public**. If you need even more reasons to join us, the first **Hip Hop Ambassador to the U.S. State Department**, Toni Blackman, will be with us to share freestyling moments across the hour.

RSVP here.

Thank you for reading.

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

Have a great, restful weekend.

The Unfinished team