Commonplace

5 Things with Matt Goerzen, Researcher at Data & Society

Matt Goerzen

Published on: May 28, 2021

License: [Creative Commons Attribution 4.0 International License \(CC-BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)

As I write this, I'm on the verge of completing two collaborative reports for my workplace, the Data & Society Research Institute. Both explore aspects of "sociotechnical security" (STsec), a security framework focused on the relational dynamics that produce exploitable vulnerabilities in sociotechnical systems, like social media, that can be difficult to identify, describe, and address through traditional security frameworks. Suitably, my five things to think about will all be filtered, to some extent, through this lens.

1. Morrowind Memes (And Recommendation Systems More Generally) as Sociotechnical Exploitation

When I open up YouTube my feed is monopolized by memetic content related to the 2002 video game *The Elder Scrolls: Morrowind*; videos where a bizarre interaction recorded on someone's cell phone is overlaid with the game's soundtrack and GUI, or where an editor has plucked the central figure of a viral video from their original context and dropped them into the game world.

Maybe you'll enjoy this selection, which sits at the top of my feed as I write this. But click it with the caveat: you might want to watch it on a throwaway account, else suffer my petty dystopian fate.

Visit the web version of this article to view interactive content.

Jumping from Vivec

For whatever reason, owing to an offhand reference made by a friend or something, a couple years ago I watched a couple videos related to the game. Now they define my YouTube experience. Sometimes upon opening YouTube I find myself engrossed by these videos, forgetting what I even intended to search for in the first place, thus fueling a vicious algorithmic feedback loop in the process.

I don't particularly find this content interesting in any way, except as a strange, longtail artifact of internet culture, and a personal demonstration of how YouTube can profoundly shape our relationship with media and, by extension, the world. Sometimes I feel like the algorithms were intentionally configured to start pushing the Morrowind memes my way around a time when YouTube was attracting criticism for its treatment of polarizing content—perhaps as part of a conscientious push to promote relatively innocuous content as a sociotechnical palliative or patch. And yet, even in this

content's innocuousness there is a view of the world presented, or maybe more importantly, a view of the world obscured.

2. D-Web as Sociotechnical Patch(?)

The developers of an emerging class of technology, often called the “decentralized web” or “d-web,” aim to break us out of platform-induced algorithmic capture. These projects steer us away from a life experience semi-determined by recommendation systems refined in deference to behavioral psychological optimizations and obfuscated profit-motivations. For example, Mastodon offers an alternative to Twitter, and there is much to think about in its move towards [community consensus-based models of moderation](#).

Yet, as d-web becomes increasingly entangled with blockchain projects and, by extension, coin-ification and speculative financialization, I find myself wondering what it will take for a decentralized web to really offer a societally preferable alternative to the web we currently have. As I become convinced that a d-web could be just as bad, equally bad, or even worse than what we have now, I crave better understandings of what the downstream implications of all of this could be.

In particular, I would love to understand how the imaginaries and visions expressed by core developers interplay with the technical affordances being instantiated and the socioeconomic ripples occasioned by the early-adopter-rewarding tools' rollout into practical uptake. I would love to better understand how a crypto-based economy rooted in a project like [Faircoin](#) could differ from one premised on those increasingly popular blockchain technologies, like Ethereum, steadily edging their way into the popular imagination through NFTs and other trojan horses.

3. Tech Secessionism as a Sociotechnical Threat

Watch the video here: <https://tknk.io/tkvu>

Advocates and developers of blockchain-related d-web projects often advance a vision of tech secessionism. I understand this to refer to the belief that technologists (Silicon Valley, or otherwise) and their user communities should strive to uncouple themselves from existing geographically-bounded state apparatuses and become more autonomous — escaping regulatory capture and taking on state-like features of their own — even as they remain geographically based within a state. While many decentralized projects are posed to make governance hypothetically easier in some ways (literally creating a distributed, unfalsifiable ledger whereby all transactions are recorded and potentially auditable) many are also posed to make the governance of technologies, their developers, and their users more difficult in other ways (facilitating forum shopping, creating data hosting mechanisms that intentionally delimit a government or company's capacity to act on content, etc.).

It's worth thinking about the way these tools, attached to visions like tech secessionism, might frustrate forms of governance that some rely on for their security. This talk, from someone involved in the finance side of blockchain, could serve as a starting point.

4. Context Collapse as a Sociotechnical Vulnerability

It's easy for keywords — even ones in a URL — to trigger the attention of an algorithmically curated monitoring feed these days. Acts of obfuscation like not using straight links or saying speaker names (notice the examples here?) can help prevent unwanted instances of [“context collapse,”](#) the phenomenon where communications framed for one audience are encountered by another, sometimes resulting in unwanted contingencies. After all, I'm writing this for you, a reader of Commonplace, not the presenter of the talk linked above, who has been known to activate networks of social media discursive combatants in bids to intentionally collapse context.

In this way, we can see context collapse, and the sociotechnical dynamics which enable it, as an example of a sociotechnical vulnerability. When users of a platform like twitter are made to worry that the content they share could be encountered or misinterpreted by unintended audiences, or outright antagonistic parties, they can self-censor. In other instances, context collapse has led to campaigns where individuals exploiting other sociotechnical vulnerabilities (like the ability to produce sockpuppet accounts) have [actively worked to undermine communities](#) by posing as members, derailing ingroup discussion, and even manipulating public perception by misrepresenting their aims.

Sociotechnical security is focused on identifying and describing these vulnerabilities, which typically fall outside of the remit of traditional security paradigms. Often these issues aren't even visible to those users the developers had in mind when they were creating their platforms—instead, they tend to disparately impact members of marginalized communities whose expertise and legitimacy in identifying these issues is

questioned or willfully ignored. Projects like [AJL's Community Reporting of Algorithmic System Harms \(CRASH\)](#) are posed to surface these issues.

5. Security by Spectacle and Bottom-Up Securitization

Finally, it's worth thinking about how issues of sociotechnical vulnerability might be addressed. Even in more established security frameworks, like cybersecurity, issues and methodologies that are now taken for granted were historically subject to contestation.

In a report I've been working on with anthropologist Gabriella Coleman, we examine ways underground hackers maneuvered themselves from being demonized, criminalized figures at the onset of the 1990s to being recognized (and often employed) as experts in computer security by the year 2000. One of the most important mechanisms they used was the production of spectacle to raise public awareness of security issues and shift the burden of responsibility for the threats these vulnerabilities posed onto the corporate vendors that developed the products.

In this way, spectacle served in a process that we call bottom-up securitization: marginal actors utilized their niche domain expertise to shame vendors, garner publicity, and direct attention to downplayed issues that were putting a growing population of internet users at risk. In this way, the hackers established the issues as security risks without direct recourse to top-down levers of institutional power.

Visit the web version of this article to view interactive content.

BO2K Presentation Behind-the-Scenes

Emblematic was the Cult of the Dead Cow (cDc)'s development and release of Back Orifice, a software that made it almost trivially easy for one user to silently commandeer another's Windows 9x machine. Trollishly framed in cDc's 1998 press release as a tool for overworked sysadmins, Microsoft responded by downplaying the insecurity of their software and instead blaming user negligence for any resulting harms. The move ignited backlash and condemnations from a growing chorus of critics, ultimately leading to Microsoft changing tact and even hiring hackers as part of their security development process in the early 2000s.

In this final video, you can watch the spectacle of the second version of the software's release at DEF CON 7 in 1999. Who are the bottom-up securitizers of our day, and what mechanisms are they using?

—**Matt Goerzen**

[Read more about Matt's work](#)