epic 2024 Ethnographic Praxis in Industry Conference Proceedings

Cybersafety in Conversation: Unifying People and Policy

COLIN MACARTHUR, *Bloom Works*
MELISSA BANYARD, *Mozilla*

Cybersecurity needs a systems update. How leaders identify and secure against virtual threats has fallen out of sync with how everyday people experience the dangers of the internet. Decision makers frame cybersecurity in dollars and cents lost, while advocates labor to humanize victims of online violence. This space lacks a common definition of safety, which is evident in the growing erosion of public trust in platforms and tech policy makers alike. In this paper, researchers from complementary ends of the cybersecurity space argue that mixed methods and ecosystems approach can lay the groundwork for improved unity between policy and people.

Introduction

The internet has grown, fractured, and repaired itself in countless ways since its inception in January of 1983 but we've now reached a pivotal moment where safety and wellbeing concerns impact broad swathes of society, not just individuals. Mass shootings at Emanuel African Methodist Episcopal Church in Charleston, South Carolina in 2015; a Walmart in El Paso, Texas in 2019; and a nightclub in Colorado Springs, Colorado in 2022 were all credited with being fueled in part by online posts that included shooters' manifestos and platforms that facilitated hate-speech, a recent report from the U.S. Government Accountability Office States indicates. And there are countless other examples of violent rhetoric and hate speech growing: Consider the rise of online groups like Libs of TikTok, who toe the lines of what platforms consider acceptable behavior, in order to dox and harass everyday people. Meanwhile, both the public and private sectors are spending millions of dollars on the development of new internet "safety" and "security" measures, even as budgets for other citizen services continue to shrink (GovTech, 2022; Google, 2023). In tandem, trust in internet services across sectors is decreasing, and a drumbeat of security and safety scandals commonly erupts across industries (Statista, 2022). So we must begin with a conclusion: The ways in which leaders identify and secure against virtual threats has fallen out of sync with how everyday people experience the dangers of the internet.

This paper was born out of a collaboration between two researchers working from opposing ends of the digital safety and security landscape. It represents not just our individual insights from our respective areas of research, but a shared realization

MacArthur, Colin, and Melissa Banyard. "Cybersafety in Conversation: Unifying People and Policy." *EPIC Proceedings* (2024): 26–44. https://www.epicpeople.org/cybersafety-unifying-people-and-policy. ISSN 1559-8918.

of the larger cracks in the foundation of the digital safety and security landscape. In this paper, we trace and attempt to reconcile the contradiction between what people need and what people get. We ask ourselves, what can ethnographers do to mend the fracture between the lived experiences of digital violence targets, and the policies developed by cybersecurity leaders?

We'll start by collectively reviewing how cyber safety and digital violence landscapes have shifted in the United States. Then, we'll present Melissa Banyard's research on the mental models and experiences of extreme targets of digital violence. The perspectives of these individuals reveal their contempt and chronic stress as they balance a need for connection with a fear of harm. Following this exploration, we then shift to the opposing industry perspective with Colin MacArthur's study of leaders within the cybersecurity space, including senior officials across the American and Italian governments. We then return to our shared birds-eye view of the problem space and propose that for ethnographers to better guide leaders towards through the development of more human policies, they might embrace the following:

- A reclamation of the concept of "value" in online security and safety policy making.
- Better supporting policymakers to create comprehensive yet dynamic maps of the ecosystem they seek to change.
- Striving to define value by observing how it gets created in the ecosystem.

In essence, this paper is a call for a disruption to the traditional ways of policy making within not just the cybersecurity space but any space in which the public and policy might interact. We believe that ethnographers have an opportunity to both empathize with and challenge leaders in order to generate more effective policies that do no harm (or at minimum, begin to better consider those they impact the most).

Shifting Foundations: Evolving Concepts of Cybercrime

From our collective experience working within policing and the private tech sectors, it's known that traditional definitions of cybercrime typically revolve around two main areas: Financial frauds and scams targeting a wide variety of individuals online (and via phone) and mass hacks or breaches. While online financial fraud is definitely growing (Wood, 2024), and cybercrime remains incredibly underreported (ISACA, 2019), the online harassment phenomenon has molded into a crisis in itself: From an American lens, over 40% of the U.S. population has reported experiencing

online harassment (Vogels, 2021). The severity of harassment is also reaching a fever pitch, with life-threatening incidents including stalking, physical threats, doxxing, and swatting (the action of making a false call to emergency services in an attempt to deploy a SWAT team to a target's home) increasing in recent years, (Belanger, 2023, Vogels, 2021, Sheridan, 2024). A survey from the Pew Research Center illustrated that the most violent aspects of online harassment (like direct threats of violence or extreme invasions of privacy) grown in frequency as well (Vogels, 2021). Those who perpetuate cyber harassment, whether they be highly motivated individuals or well-organized groups, often attempt to remove a target's privacy or damage their reputation, removing their sense of well-being and self-worth in the process. Malicious intent, often fueled by gender and racial bias, is at the core of many doxxing instances, especially within the United States, (Eckert and Metzger-Riftkin 2020). Contributing factors like more of our lives and livelihoods taking place online, the volatile nature of American and global politics, and ever evolving legal conditions are all ever-present as well.

In summary, we're witnessing an undeniable uptick in a type of cybersecurity threat unique unto its own. What separates national security threats, corporate hacks, and financial fraud from this emerging category, is how deeply emotionally impacted individual targets are, as well as the acute threat on individual's lives and livelihoods. Finally, as this problem escalates, individuals who might be presently unimpacted by online harassment but increasingly aware of the volatile nature of internet communities are voicing their concerns. Motivation amongst the general population to address this problem is growing in tandem, with 93% of adults expressing slight to extreme degrees of concern with "compromise of personal information" (incl. Address & phone number) being a top concern (Sheridan, 2024).

In light of these escalating issues, Melissa Banyard, alongside a co-researcher at Mozilla, Alice Rhee, facilitated research focused on identifying strategies to support victims of digital violence. This research, conducted with the aim of developing effective cybersafety and cybersecurity solutions, leveraged firsthand accounts to gain insights into the experiences of individuals affected by these forms of abuse. This ethnographic approach provided a foundational understanding, revealing participants' fears, mental models, and key needs whilst coping with online harassment.

Research Methodology for the Study of Digital Violence

The first-hand research described in this section was deployed with the original intention of identifying opportunities to support victims of digital violence, on behalf of the Mozilla corporation. The core activity in this research involved showing

participants, in a one-to-one setting, samples of possible cybersafety and cybersecurity-related technology solutions. Participants were asked to provide direct feedback on these concepts and force rank them against each other to surface insights that a team of designers and developers might act on. In order to build a foundational understanding of the experience of online harassment and doxxing, the researchers (this paper's author, in tandem with Alice Rhee, another design researcher at Mozilla), embedded an ethnographic approach within these feedback sessions. They did this by beginning the session by asking participants to describe a significant experience with online harassment, cyber-stalking, or doxxing. From there, they explored themes regarding the participants' fears and concerns, their key actions before, during, and after an event, and finally, their concept of personal resiliency and recovery from online violence. All conversations took place virtually and lasted between 30–90 minutes.

Participants over 18 were selected if they met two main criteria:

1. They were working professionals within North America or Europe. For many participants, the professions they were part of or the subjects they dealt within their work would be considered "contentious" within the context of 21st-century Western Culture. The co-researchers actively recruited journalists, health care providers working within gender-affirming care, planned parenthood, or abortion providers, and community leaders like municipal politicians.
2. They had experienced some form of direct online threat or digital violence to either themselves, their workplace, or their close colleagues. Some of these attacks were semi-organized by online groups (cyberbullying groups, semi-political organizations), while others were attacks from individual cyberstalkers or groups of 2–10 people.

Participants had varying degrees of exposure due to their attacks: In most extreme cases, participants described moving to new towns or countries or having their stories picked up by "alternative" and mainstream news outlets. Their experiences were often insightful but devastating, and the opportunity to speak with targets of digital violence one-on-one, in a safe manner, brought forth many more details than what we could garnish from reading written accounts, or following events in forums or public interviews. With respect, this author notes the incredible resiliency and activism of all participants interviewed.

Finding 1: Platforms Are Failing to Regulate Hate Speech, and People Can Tell

The majority of our research participants within this first study expressed that they explicitly believed that current measures to prevent threats and harassment on platforms were ineffective. Throughout discussions regarding a platform's ability to block or prevent the spread of violent language, whether it was general or targeted at individuals, many participants conveyed a lack of trust in the platform's capability to take action against violent rhetoric. One participant mentioned that platforms don't block attackers "because [platforms] will get into conversations they don't want to have." They felt that leaders and safety teams within social media companies were actively avoiding wading into the complexity required to solve clashes between individuals on their platforms.

Most notably, participants who were established professionals in "contentious" areas like reproductive health or those who worked in semi-public capacities like published writers were also highly attuned to the subtleties of language that could come across as abusive yet did not actually violate the official rules and guidelines established by social media platforms. These individuals reflected on how difficult it is to clearly define "abuse" within the social media context and questioned the ability of social media companies to establish safe spaces without impinging on free speech.

Concerns sounded like:

> "What counts as abuse? That can be tricky. The messages I tend to get are like 'you're going to hell…' [but] they're not exactly threatening…"

And from another participant:

> "Blocking strategies work better for grooming and revenge porn than they do for extremism. A lot of [hate speech] is coded and cloaked so the AI doesn't pick it up."

Most importantly, participants described how organized harassers (like online hate groups or serial stalkers) exploited loopholes in the rules. They used subtle threats or language that barely stayed within acceptable limits. This led participants to lose confidence in the reporting mechanisms on social media platforms for curbing abusive content. Many attempted to block individuals but found it ineffective as new fake accounts or "sock puppets" would reappear, especially when dealing with well-organized hate groups. Participants also found that blocking and reporting harassers often proved pointless, as the abuse would still occur elsewhere in the online community.

In a paper published in the Fordham International Law Journal in 2018, the author compares German and American hate speech laws (the former's laws being largely regarded as more protective and respectful within privacy and security circles), and states that German hate speech laws often prioritize dignity, while American hate speech laws prioritize liberty. In our time spent with these targets of severe online harassment, we witnessed the fallout, the consequences essentially, of lawmakers and social media platform leaders who prioritized "freedom of speech" and connectivity without also considering how they'd preserve the wellbeing and dignity of even the most vulnerable users on their sites. Our participants called out that social media guidelines and state or national laws protected against explicit threats, but not implicit ones, and prioritized freedom of speech over the individual's right to peace.

Relatedly, when prompted further on this subject, some of our study participants even expressed the feeling that platforms were actively promoting violent rhetoric. Some felt that platforms not only fail to remove abusive content but that their algorithm actually rewarded abusers with engagement. They pointed to an increase in violent or misogynistic language on their social media accounts, despite their attempts to block or report content, as evidence. One participant told us, "They're facilitating hate, yet they don't do anything to stop [the harassment]".

The fact that social media often fosters abuse or calls for violence against individuals is not just a perception but a confirmed reality. One possible reason for this phenomenon is the conflicting priorities between the concerns of platform users and those of advertisers (to whom executives are beholden to). Advertisers, as the direct source of revenue for platforms, often have more influence over moderation policies and practices than average users (DeCook et al, 2022). DeCook et al also point out that AI and automated abuse detection systems are not always effective in identifying more subtle forms of abuse, which aligns with the frustrations expressed by our research participants.

Finding 2: Retreating is Not the Answer

So, if the internet is growing more unstable, more violent as the years go by, why don't people just leave? Step off these platforms, hide themselves and their families? Traditional advice in this area from law enforcement, and cyber-safety consultants is often to take a "locked down" approach: delete profiles, throw away devices, change your locks. Contrary to this, many of the participants we interviewed, especially those working in women's health, LGBTIQA+ rights, or other areas of activism, found it

necessary to maintain an online presence even in the face of ongoing harassment. It's essential to recognize that it's not only journalists and politicians who require public platforms to express their views and share their work. Professionals in fields such as climate science, education, and public health also need to be online to ensure that critical information is available and accessible. Many participants acknowledged this requirement in their work, and the risks they chose to take on in order to perform their activism and public communication well. They also expressed a strong connection to their respective online communities, particularly if they identified as women in male-dominated fields, members of the LGBTQIA+ community, and / or people of color.

When confronted with harassment or a sudden increase in abusive behavior, participants continued to be active on the very platforms where they were targeted to maintain their online reputations, carry on with their work, and assess the severity of threats made by the harassers. In fact, very few of those who we interviewed retreated completely or permanently from the internet following a bout of harassment or violence. This was in part due to the reasons stated above (a need to remain online for work and a desire to connect with communities) but also for safety reasons. One participant shared with us:

> "If someone is talking about you… you sort of have to know about it. So in a situation where people are talking about you… you go down a rabbit hole of wanting to see [the harassment] because you're trying to get ahead of the situation. The anxiety kicks in when you're trying to stay ahead of this wave of nonsense... But you're also reading some really terrible things about yourself. There's this fear that something bigger is going to be said… are they going to find pictures of me as a teenager? What are they going to do with that information?"

While some people chose to leave online communities, the majority remained in order to stay informed about what was happening. This need to remain aware of the situation was accompanied by feelings of burnout, fear, or extreme anxiety, which affected the quality of life for both individuals and their communities.

However, it's important to note that some people found positives amidst this chaos. Those who felt exhausted and frustrated by the platform's failure to stop violent language also had the potential to feel a sense of resilience in surviving these attacks. They developed a sense of pride in their new roles as defenders of their beliefs and identities online. And this pride, strengthened their resolve to fight for their causes, strengthened their sense of their identity being tied to certain values, and improved or created new connections to community members experiencing similar harassment.

Foundations at Risk: The Healthy Internet

The perspectives outlined above are only intensifying, especially in the ramp-up towards the 2024 U.S. election, and other major world events. The growing disparity between individual cyber safety needs, law enforcement capabilities, and the policies enforced by mainstream platforms underscores a critical challenge. As our identities and lives become increasingly intertwined online, the most nuanced aspects are exposed to risk. Citing DeCook et al. once again (2022), while categorizing types of harm is crucial for moderation efforts, platforms often fall short in addressing the root causes of harmful behaviors and content. This failure jeopardizes both personal freedoms and our right to privacy, as algorithms prioritize engagement over these fundamental rights. Targets of digital violence frequently find themselves overlooked when their experiences challenge existing platform rules, and the impact of harassment is not easily quantified or measured. These complexities highlight pressing questions about how to mitigate unmeasurable phenomena such as "feeling controlled" or "feeling watched."

There's a question unanswered at this point in time: Why should platforms police individuals? Is that not a job for law enforcement? In our previous experience within the Royal Canadian Mounted Police's Cybercrime Coordination Unit, one of the authors of this paper also personally witnessed a lack of existing infrastructure within policing to meaningfully support victims of online harassment. In many cases, officers were limited by two key things: A lack of strong evidence of a real threat and a lack of resources and training to prevent digital violence. Other exacerbating factors like systemic racism, sexism, and homophobia were also at play and this is a widespread policing phenomenon: "Systemic racism, sexism, and homophobia among police officers contribute to disparities in policing practices, including biases in who receives assistance and who is ignored." (Harris, 2020). Existing analyses of digital violence cases outside of our first-hand research confirm that particularly in cases of doxxing, law enforcement and social media providers rarely provide meaningful next steps and support (Eckert & Metzger-Riftkin 2020). Addressing the challenges of online harassment demands not only improved infrastructure and resources within policing but also a concerted effort to combat systemic biases that perpetuate disparities in victim support and response strategies, as well as a need to wholeheartedly address policy decisions made within social media companies. To address this problem we must instead first acknowledge its complexity. No one institution can resolve this issue in a silo.

Creating healthier online communities is also an important part of the solution, and there have been numerous efforts in recent years to explore and develop new spaces for meaningful discussions online (Chedraoui, 2024). However, alternative platforms like Mastodon and Cara, while existing on the fringes, have not attracted the same level of attention and user base as mainstream social media platforms, which have a "stickiness" to them (by design). While we hope to see these emerging platforms grow in a healthy manner, there is also an opportunity for researchers to challenge and influence the way traditional institutions approach cybersecurity. There is potential to re-evaluate platform governance in the wake of the disruptions referenced earlier in this paper…and establish new ways of approaching this growing problem of online harassment.

Ultimately, leaders and everyday people need shared values and conceptualizations of the problems they're trying to avoid and fix. No easy feat, so before we jump into solutions, let's start by looking at the other side of the conversation: towards the viewpoints of policymakers and leaders within the cybersecurity space. How do they conceptualize the problem of online safety? And how might we begin to overlap their conceptualizations with those of victims of digital violence? Finally, how can ethnographers help leaders towards better platform governance?

Why Violence Happens: Leader Conceptualizations of Security and Safety

We might begin by asking "How does platform governance actually happen?" Although we know that governance is a complex phenomenon, with both implicit and explicit mechanisms, there are often certain key individuals in shaping a platform policy. We call these people "leaders". Leaders are the people who influence the rules platforms set, the norms they apply, and the enforcement mechanisms they create. What is the real goal of the platform and platform security? What do the key terms in these goals mean? Although leaders may all apply similar socio-technical tactics, their underlying conceptualizations of security may well differ substantially.

The leaders who influence cyber space, its safety and its policy can be found in many places. Of course, the leaders of the companies that build and maintain social media come to mind first. But these people also exist within a web of influence from others. For example, government leaders set rules and make pronouncements that create constraints and goals for platform companies. Academics, too, are "leaders" in the space – they often suggest mechanisms (combined rules, assumptions, and roles) that industry and government leaders adopt.

Thus, to understand how platform governance really happens, we looked to leaders in tech companies, government agencies, and academia. We aimed to understand not just the policies (and how they are set and approached) but also the underlying definition of security that sets the ground for their approach.

Research Methodology for Study of Cybersecurity Leaders

Between August 2022 and May 2023, one of the authors and his collaborators conducted extended interviews with 31 leaders who work on issues of digital safety and security. These leaders came from governments, academia, and the private sector. We sought leaders from both the United States and Italy, where the authors were based.

Our interviews included senior officials in the United States and Italy's national government. Several of these officials were senior advisors for policy making or planning in each country's cybersecurity agency. Others were responsible for education and training in each country's technical institutes. We found these leaders by approaching each country's security and IT agencies and asking for senior officials interested in speaking about cyber security or safety policy making with leaders. We also interviewed several U.S. state-level cybersecurity leaders, including the state Chief Information Security Officer from several states.

We approached leaders from each of the major platforms identified by the European Digital Services Act. We deliberately attempted to speak with people from both the American central policy-making circle and others. In the end, we often spoke with VP-level security and safety officials from several of these companies, although they explicitly required the companies themselves to remain unnamed.

Finally, we also approached and interviewed academics whose work is influential in private and public sector governance. We largely found these leaders through recommendations from private and public sector leaders. We also conducted a large literature analysis (not reported here) that surfaced several

We met leaders in their offices or invited them to a workshop planned for Milan, Italy. The interviews were semi-structured and ranged from 30 minutes to 3 hours. They covered topics like the leaders' personal definitions of cybersecurity or safety, their current focus, the concept of key players, and common challenges.

This work was funded by a grant from the U.S. Mission to Italy. Excerpts from many of the interviews can be found on the "Cybersecurity for Public Value" podcast, where some interview recordings have been republished with permission.

Failures of Generation: The Very Narrow Definition of Safety and Security

When we asked leaders how they defined "cybersecurity" or "safety," we often received blank looks. These words are so commonly used and treated as self-explanatory that almost no one could articulate what their "target" was.

When they did try to articulate it, many moved away from defining safety or security and towards sharing the actions necessary to accomplish it (whatever "it" is). For example, they described the rules they were trying to implement in their organization or particular technologies they wanted adopted state-wide. Sometimes, leaders would talk about the other things that safety and security would enable. For example, if a system is secure, the company can continue to profit from it, and the users can continue to use it.

When leaders shared the desired effects of cyber safety and security, they got closer to telling us what they thought cybersecurity really was. For the majority of interviewees, cybersecurity and safety were:

- **Aimed at organizational self-preservation.** In other words, they were about keeping their organization alive and functioning. For private sector leaders, this often meant making money (and maintaining the reputation necessary to make money). For government leaders, this often meant avoiding scandal that lessened government trust (and led to sudden leadership change).
- **Supporting other organizational processes.** Attaining "security" or "safety" were never goals in and of themselves. They were rather important measures to ensure that other parts of the organization. For example, government leaders spoke about ensuring the "safety" of critical business processes, like mailing important letters or depositing checks. Business leaders talked about the "critical customer journeys" that are essential for governments to continue to make money.
- **What could be "easily" – quantitatively – measured.** We noticed (as did our interviewees) that describing cybersecurity in terms of preserving organizations and their processes was easy to measure. "Either we're online, or we're not," as one participant mentioned to me. And whether existing processes are operational and speedy can also be easily quantified. In other words, there was a pull toward.

In other words, the security and safety that leaders aim for is ultimately what's simply measurable: whether the organization and its processes live or die.

Sometimes, they move a degree away, by considering whether reputation or organizational trust could disturb the organizations and their processes.

We have generally not separated leader discussions about cyber "safety" and "security" here. That is purposeful. For both, the operationalization is about the same. Although leaders interviewed might lean more on organizational reputation when considering safely, their ultimate goal is still measurable organizational self-preservation.

Myopias of Cyber Safety and Security Governance

What happens when leaders start to influence policy based on these implied definitions? We believe victim frustration can be directly tied to how leaders conceptualize these terms. Deciding what security and safety actually mean – or even what behaviors they enable – are not theoretical exercises; they have real impacts on individuals' lives, feelings of safety, and sense of autonomy.

Much is lost by conceptualizing security and safety in such a limited way. There's nothing wrong with considering organizational preservation and what's easily "measurable" while influencing governance. The problem is when little else is considered and how those limits trickle into the policy-making at hand.

For example, when they consider organizational preservation, leaders often ignore the preservation of other entities in their orbit. Leaders of tech companies did not mention the preservation of their democratic societies as a key value at hand. Public sector leaders likewise often did not talk about the preservation of their capitalist partners. As a result, their governance process evaluates possible courses of action against existential threats to their organization but not necessarily to others.

There's a deep irony in this myopia: the internet has created these organizations, these threats and tied many private sector actors and governments deeper together. Each's existence depends on the other. In their attempt to preserve themselves, they may undermine everyone else they depend upon.

The myopic focus on protecting essential "business processes" leads to similar mistakes. Business leaders are so focused on recognizing particular routines or activities to be protected that they miss other views of an organization. For example, one leader mentioned that he never realized there was a "psychosocial element" of organizational response to a cyber threat or attack. In other words, even when the systems responsible for the business kept running, their operators might be shocked or overwhelmed by the risk. The emotional resilience of his employees was essential – but none of the organization's policies acknowledged this.

As most ethnographers know, an obsession with what's countable – on etic questions – leads to predictable blind spots. For leaders of cyber security and safety, this amplifies the problems of other myopias. Because leaders prioritize what can easily be measured in numbers, they are unlikely to notice the less tangible but important ties they hold with other organizations. Because they focus on processes that have a countable output, they fail to conceive their organizations in any other way.

Another way to describe these myopias is a failure to comprehensively assess value-at-risk. Value-at-risk is a financial term for how much the value of an investment could lose if market conditions change. Financial risk management is obsessed with creating a comprehensive picture of the value-at-risk for a company from many angles and given many interconnections. Interestingly, as several leaders pointed out, most organizations (public and private) don't do the same thing when it comes to setting safety and policy governance on their platforms. An organization's finance department probably does a better job at assessing what could really be lost than its "cyber risk" department.

Frustrated Leaders: An Opportunity for Displacement and Generation

Despite these myopic approaches to governance, leaders themselves offer hope of change: their own frustrations with the limits of their own governance processes. Indeed, they actively seek to displace their existing myopias and take generative approaches to new policymaking. Prodded by academics in their orbit, several leaders noted there were obvious limits to their processes. As one private sector leader shared:

> "Look, I know there are many things we're missing. I just can't find a way to systematically manage them all without going nuts. I wish there was a way to think more broadly, but I have 10 fires on my desk."

Some leaders noted that they have tried to "widen the lens" of their safety and security governance. Sometimes, they explicitly charge their governance groups with considering the societal risks their platforms provide, only to get "blowback from shareholders." Sometimes, they encourage taking the viewpoint of victims of violence on platforms but struggle to systematically manage them the way they do "essential business processes." They certainly feel cybersafety and policy governance have ample room for improvement.

Conclusion: Using Ethnography to Displace the Old "Cybersecurity" and "Cybersafety"

We believe that ethnographers can help craft better, more human-centered policies within the cyber safety space. There are many already doing so, like Susan Squires and Molly Shade (2015), who spoke on the importance of identifying gaps between policy as it is written and policy as it is interpreted by individuals across a variety of professions: "Dourish and Anderson (2006) point out that individual risk perception is embedded in a context of language, rhetoric, values, norms, and cultures shared with other members of their work community or group." From our collective research and experience, we know with confidence that leaders in the public and private sectors tend to heavily rely on statistics and quantitative evidence to commit to change within cybersecurity areas. Governance is an opportunity for mixed methods application: we don't expect leaders to abandon their graphs and numbers; we just hope to deepen and widen their conceptions of security and privacy.

Drawing on the work of participatory public administration researchers, we propose that ethnographers aiding security and safety policy making:

Ethnographers Should Explore the Concept of "Value" in Online Security and Safety Policy Making

For massive online platforms and the governments regulating them, value is not simply profit lost or GDP gained. We draw inspiration from Moore's (1995) work, which articulated that policymakers and leaders have a responsibility to create something "substantively valuable for the society" and can do so by following a feasible, sustainable, and legitimate strategy (p. 71). Policymakers can (and should) derive value by creating policy that orchestrates the interconnected actors. They need to discover all of the forms of value their organization wants to protect (including those not related to the organization itself). And that starts with a more comprehensive view of their environment. In order to do so:

Ethnographers should use their tools to help policymakers create a comprehensive, dynamic map of their ecosystem

The ecosystem includes all the values, organizations, individuals and behaviors in their orbit (Osborne et al, 2021; Akaka et al, 2013). In particular, ethnographers aiding organizational policy-making should use interviews, workshops and other

participatory methods to identify how several different possible "targets" of policy-making connect together (as adapted from Osborne et al, 2021):

- **Macro-level**: the societal values and institutional norms related to the organization and its domain
- **Meso-level**; the other public and private organizations in the domain and the relationships and technologies that connect them together
- **Micro-level**: types of single individuals, like victims or content creators, that relate to those organizations
- **Sub-micro level**: the particular behaviors of individuals as they interact with each other or those organizations

Organizations Should Define Value by Observing How It Gets Created in the Ecosystem

Instead of hypothesizing and assuming about when and how organizations and individuals work together to create "safety" and "security," we should seek the places where it actually happens. In other words, instead of defining safety from the top down, we should define it based on where individuals see it happening in the system. And we should look not just between typical relationships, like technology provider and user, but at those all around.

The Ecosystem Approach to Cyber Safety in Practice

There are already promising signs that some government agencies and platforms are adopting elements of this approach in their policymaking. In our interviews, one government agency responsible for elements of internet policymaking had recently begun a new strategic planning process. At the beginning of their process, one of the senior leaders shared his slogan: "No assumptions!" He explained that he wanted to carefully examine the agency's role in making the internet safe and secure and avoid previous simplistic assumptions about the key goals. To re-examine assumptions about policy goals, the agency's leader invited people with various perspectives about the agency's role on the internet to share their perspectives on questions like "What's most important to protect?" and "How do we make lives better?"

Their answers fell into the categories described above:

- **Macro-level**: Some of the attendees spoke to the ways that the agency advanced societal values. One spoke about how the internet allowed "people to create their own destinies," invoking individualism. Another spoke about how the internet advanced "productivity in safety."

- **Meso-level**: Others spoke about how their organizations and collaborations with the agency enabled their work to continue. Interestingly, they also often talked about organizations that did not interact directly with the government agencies, but were benefited by their actions second or third hand. One speaker conjured the "network of institutions, not computers" that compose the internet.
- **Micro-level**: Happily, there were also people without institutional connections in the group. Some of them were people who had created individual small businesses on the internet; others were "content creators" who benefitted from the advertisements that appeared next to their products. Each of them discussed how their individual livelihoods depend on the internet.

In other words, the discussion identified actors or values created at many different levels of the internet. In subsequent months, the senior leader kept reminding the strategic planning team of this discussion and returning to the levels and types of value described. He encouraged them to consider how various regulatory measures protected the value described at different levels. For example:

- The strategic planning team noted that much of their existing regulation and advice about computer and network configuration served only the "meso-level," and only part of it at that. It tended to only contemplate the organizations that were directly affected by the team's rules and focused on ensuring their ongoing survival under different potential threats. However, the planners noted that organization-targeted regulation had many "ripple effects" on other entities. For example, requiring organizations to adopt certain approaches to authentication strengthened the government agency's interactions with them but made it harder for those organizations to do business with their partners.
- The senior leader also noted that almost none of the agency's programs were targeted at protecting the "micro-level." Those people who depended on the internet, but were increasingly dubious about whether the government and platforms wished to protect them (as mentioned earlier in this paper in our interviews with targets of digital violence). The few individual-level programs were focused on behaviors. This realization forced the leader to consider how organization-targeted regulation might be reshaped to protect individuals (not just organizations themselves). He said:

> "I still have an image in my mind of [meeting participants] tearfully talking about what they would lose if [platform] changed their rules, even if that platform still exists."

- Above all, the planners increasingly returned to the societal values (beyond "keeping governments and related organizations productive") their work promoted. Several remarked that they realized the role their decisions played in maintaining the country's approaches.

Although a relatively haphazard set of realizations, these set in course a less "myopic" policy process at this agency. This process inspired the authors to consider how ethnographers could further enrich conversations about "what's at stake" on the internet and in turn prompt organizations to be less myopic.

Final Note: Ethnographers Deserve a Seat at Policy Tables

If nothing else, we hope the preceding research and these examples show how qualitative methods can contribute to security and privacy policy-making. Cybersecurity and "security studies" rarely use ethnographic tools, and ethnographers often cede this topic to the "technical people." We provide a counterexample.

Ethnographic approaches are not just useful for shaping websites, apps, and tools (as is often discussed these days) but also for the bigger ideas that guide institutions and their policies. Ethnographic research can enter the "strategic level, not just in shaping what products are built, but how our internet is stewarded. Perhaps the authors' collaboration can serve as a small example. Although we had worked together in the past, we conducted the two projects described here separately. Each brings a different lens to cybersecurity and safety, and combines them to propose a different way to widen the perspective of policy makers.

About the Authors

Colin MacArthur is a leader in user experience research and design for public sector services. He is currently an engagement manager at Bloom Works, a public benefit corporation dedicated to building better digital public services.. Previously, he was the first Director of Digital Practice and Head of Design Research at the Canadian Digital Service. He was also an early team member at 18F and the Center for Civic Design.

Mel Banyard is a researcher in tech with a focus on privacy, cybercrime, and digital violence. She's passionate about creating sustainable change within the organizations that shape our online lives. At

Mozilla, she studied the growing rate of doxxing and online harassment against professionals in the United States & Mexico. Prior to that, Mel led mixed-methods research for the Government of Canada's COVID Alert App and the Royal Canadian Mounted Police's Cybercrime Reporting Platform.

References Cited

Akaka, Melissa Archpru, Stephen L. Vargo, & Robert F. Lusch (2013). The Complexity of Context: A Service Ecosystems Approach for International Marketing. *Journal of International Marketing 21*(4): 1-20.

Asher-Schapiro, A., & A. Moloney (2023, August 1). US Abortion Advocates Face Doxxing as Data Scavenged Online. Thomson Reuters Foundation. Retrieved July 1, 2024, from https://www.reuters.com/article/business/healthcare-pharmaceuticals/feature-us-abortion-advocates-face-doxxing-as-data-scavenged-online-idUSL8N39E8D3/

Belanger, A. (2023, June 30). FBI finally Tracks "Swatting" Incidents as Attacks Increase Nationwide. *Ars Technica*. https://arstechnica.com/tech-policy/2023/06/fbi-finally-tracks-swatting-incidents-as-attacks-increase-nationwide/

Chedraoui, K. (2024, May 30). How We're Bringing Back the "Social" Part of Social Media. CNET. https://www.cnet.com/news/social-media/how-were-bringing-back-the-social-part-of-social-media

DeCook, Julia R., Kelley Cotter, Shaheen Kanthawala, & Kali Foyle (2022). Safe From "Harm": The Governance of Violence by Platforms. *Policy & Internet 14*(1): 63–78. https://doi.org/10.1002/poi3.290

Eckert, Stine, & Jade Metzger-Riftkin. 2020. Doxxing, Privacy and Gendered Harassment. The Shock and Normalization of Veillance Cultures. *Medien & Kommunikationswissenschaft 68*(3): 273–87. https://doi.org/10.5771/1615-634x-2020-3-273

Harris, D.A. (2020). Systemic Racism, Sexism, and Homophobia in Policing: Toward Justice and Equality. Routledge.

ISACA (2019, June 3). New Study Reveals Cybercrime May Be Widely Underreported—Even When Laws Mandate Disclosure. https://web.archive.org/web/20230615155408/https://www.isaca.org/about-us/newsroom/press-releases/2019/new-study-reveals-cybercrime-may-be-widely-underreported-even-when-laws-mandate-disclosure

Levine, Deborah (2018). Sticks and Stones May Break My Bones, but Words May Also Hurt Me: A Comparison of United States and German Hate Speech Laws. *Fordham International Law Journal 41*(5): 1293. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2720&context=ilj

Moore, Mark H. (2015). Creating a Public Value Account and Scorecard. *Public value and public administration*, 110–130.

Nasi, Greta & Colin MacArthur (Hosts). Cybersecurity for Public Value [Audio Podcast]. Bocconi University. https://www.unibocconi.it/en/news/cybersecuring-countryaeu-podcast

Osborne, S. P., G. Nasi, & M. Powell (2021). Beyond Co-production: Value Creation and Public Services. *Public Administration 99*(4), 641-657.

Sheridan, M. (2024, August 8). Doxxing Statistics in 2024: 11 Million Americans Have Been Victimized. SafeHome.org. https://www.safehome.org/family-safety/doxxing-online-harassment-research/

Vogels, Emily A. (2021, January 13). The State of Online Harassment. Pew Research Center. https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

Wood, J. (2024, April 10). 'Pig-Butchering' Scams on the Rise as Technology Amplifies Financial Fraud, Interpol Warns. World Economic Forum. https://www.weforum.org/agenda/2024/04/interpol-financial-fraud-scams-cybercrime/#:~:text=Financial%20fraud%20is%20increasing%20worldwide,Criminal%20Police%20Organization%20