# Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity

JAMES PIERCE, University of California, Berkeley, USA
SARAH FOX, University of Washington, USA
NICK MERRILL, University of California, Berkeley, USA
RICHMOND WONG, University of California, Berkeley, USA

We investigate cybersecurity toolkits, collections of public facing materials intended to help users achieve security online. Through a qualitative analysis of 41 online toolkits, we present a set of key design dimensions: agentive scale (who is responsible for security), achievability (can security be achieved), and interventional stage (when are security measures taken). Recognizing toolkits as socially and culturally situated, we surface ways in which toolkits construct security as a value and, in so doing, how they construct people as (in)secure users. We center the notion of *differential vulnerabilities*, an understanding of security that recognizes safety as socially contingent, adversaries as unstable figures, and risk as differentially applied based on markers of relational position (e.g. class, race, religion, gender, geography, experience). We argue that differential vulnerabilities provides a key design concern in future security resources, and a critical concept for security discourses.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy** • Social and professional topics → Computing / technology policy → Computer crime → Social engineering attacks

**KEYWORDS**

Cybersecurity; differential vulnerabilities; values in design

**ACM Reference format:**
James Pierce, Sarah Fox, Nick Merrill, Richmond Wong, 2018. Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. In *Proceedings of the ACM on Human-Computer Interaction,* Vol. 2, CSCW, Article 139 (November 2018). ACM, New York, NY. 23 pages. https://doi.org/10.1145/3274407



## 1 INTRODUCTION

In October 2014, feminist media critic Anna Sarkeesian was set to give a lecture at Utah State University. In the months and days leading up to the scheduled talk, attackers sent Sarkeesian rape and death threats, hacked her social media accounts and websites, vandalized her article on Wikipedia, and distributed personal information such as her phone number and home address (a practice referred to as doxxing). Ultimately, Sarkeesian was forced to cancel the event after a bomb threat. Sarkeesian's, among many other stories of cybersecurity attacks, foreground a key question: What can people *actually do* to achieve security online?

*Authors contributed equally to the paper. A random number generator was used to help decide author order. Each author is thus a lead author of this work.


2573-0142/2018/November – ART139 $15.00

https://doi.org/10.1145/3274407

To understand how issues of cybersecurity are currently being addressed and framed, we study a class of public-facing technologies and documents we refer to as "cybersecurity toolkits"—online collections of tools, tutorials, and tips aimed to help individuals or groups improve their security online. Many toolkits focus on the needs of specific groups, including those described as having particular, acute security vulnerabilities such as journalists, activists, religious minorities, and members of LGBTQ communities. Yet toolkits are not always designed, curated, and distributed by members of these groups. Instead, they are created and maintained by a diverse range of organizations with many different political orientations and ethical commitments, ranging from the US Department of Homeland Security, to the Electronic Frontier Foundation, to Sarkeesian's own Feminist Frequency.

We argue that cybersecurity toolkits surface critical security needs not met by mainstream institutions (e.g. service providers, governments, manufacturers). Drawing on a values in design approach, we seek to understand how these toolkits construct and promote the value of "security" such that certain users are seen as insecure and particular threats become salient and thus amenable to defense. Through this frame, we aim to answer two main questions: First, what can we learn about security from the design and rhetoric of cybersecurity toolkits? Second, how might these understandings inform both broader theoretical and critical discourses on security and the design of toolkits (from formulating actionable recommendations to proposing experimental alternatives)?

In addressing these questions, we extend discussions on inclusivity in cybersecurity [30] to consider the variable threats and harms uniquely directed at those who sit on social or political peripheries, such as those facing religious, gender, or racially-motivated attacks. From our empirical analysis, we introduce the notion of *differential vulnerabilities*, a concept that recognizes how different populations face different types and degrees of security risks. This notion joins in challenging universalizing tendencies that frame cybersecurity around an abstract or generic user [13]. We discuss differential vulnerabilities both as a pragmatic design concern and as a critical concept for broader security discourses, contributing a set of key design considerations useful for analyzing current cybersecurity toolkits and synthesizing possible alternatives.

## 2 RELATED WORK: APPROACHES TO SECURITY

We first review CSCW, HCI, and related fields' responses to user-centered approaches to security, incorporating notions of security as a sociocultural practice. We then discuss social values-oriented approaches to design and how these perspectives inform our analysis. Finally we discuss recent work that considers how interfaces and technologies construct users, and how cybersecurity toolkits differentially formulate users as insecure and in need of security.

### 2.1 Responses to User-Centered Approaches to Security

Since Tygar's study on the usability of PGP encryption [31], usable security research has sought to understand the practice of security through user-centered design [e.g. 12, 26]. Such approaches tend to focus on how to ease the process for users seeking to achieve technical security. For instance, researchers redesign security settings and notices to be more usable, create third-party tools to assist in security decision-making, or build secure architectures and design patterns.

Several critiques have complicated these approaches. Dourish and Anderson reconceptualize security (and privacy), "not simply as technical phenomena but as embedded in social and cultural contexts," and entangled within broader rhetorical strategies, practices, and politics, such as those

around risk, trust, and morality [11:319]. The authors discuss security as a practice in which "privacy and security are continual, ongoing accomplishments; they are constantly being produced and reproduced," [11:283]. Dourish and Anderson thus suggest that security needs to be investigated through the study of everyday practices. Similar concerns about the sociocultural aspects of security have also been raised within technical security communities, such as concerns about usable security's construction of a normative end-user, or obscuration of the social positionality of security practitioners [13, 30]. Wang, for example, suggests that security research needs to consider and include a broader range of user abilities and experiences [30].

Recognizing security as socioculturally situated, prior empirical research in CSCW and related fields has tried to better understand how people situated in specific contexts conceptualize and construct their security or lack thereof. This work includes studies of photo sharing by users in Saudi Arabia and Qatar [1], teenaged social networking users [18], or domestic labor practices to implement and maintain online security in Silicon Valley household settings [27]. Other CSCW work has studied practices and behaviors surrounding the adoption or lack of adoption of security-related tools and features by users and developers [9, 34].

Building on Dourish and Anderson's reframing of security, we complement these studies by focusing on the rhetorical and discursive practices of a range of security-related artifacts—cybersecurity toolkits—to understand how these toolkits work to frame security and those in need of it. Toolkits suggest how different groups should see themselves and one another as vulnerable to particular sorts of threats. For example, toolkits on doxxing tend to focus on the practices and experiences within communities such as 4chan, which is home to many trolling groups. In other words, our investigation is concerned with the practices and conceptualizations that toolkits put forth in name of security. To conduct this analysis, we turn to a set of lenses within CSCW that note how seemingly "neutral" practices and artifacts, in fact, contain and support particular politics and social values.

### 2.2 A Values Approach to Security

Prior research within CSCW, Science & Technology Studies (STS), and related fields has considered how technical practices and computational artifacts promote or embed particular social values [14, 16, 23, 32]. These research programs offer both understandings of the political nature of technological devices [32] and lay important theoretical groundwork for bodies of designed oriented work prominent within CSCW and HCI more broadly, such as "values in design" [19, 23] and Value Sensitive Design [14]. Here, through careful collaboration and consideration of stakeholder positions, a technical system may be designed in ways that are compatible with or responsive to the values of those intended to use it [14, 19, 23]. Recent work has moved away from considering values as stable, universal phenomena, instead seeing values as instantiated through specific practices [10, 16, 21, 29], or as Houston et al. describe, "a more fluid and emergent model that treats value as an active and ongoing *process*" [16].

With respect to security, Helen Nissenbaum discusses differences in how the traditions of national security and computer science approach issues of cybersecurity. Nissenbaum, for example, notes differences in how these two distinct security traditions formulate security threats, conceptualize the objects that get protected by security, and articulate the moral justification for security [24]. Building on the term *securitization*, which has origins in the fields of security studies and international relations, she describes the practices that government and corporate actors use to characterize what and why something is a security threat, and the appropriate measures to respond to the threat. These perspectives together highlight that security as a value is not universal and unchanging; rather security is supported and constantly being

made by local sociocultural practices that characterize who and what is deemed "secure" or "insecure."

Informed by work related to "values in design", our work investigates security toolkits with attention to the relationships between design, use, and social values. In particular, we are interested in the social values reflected in and propagated through security toolkits. Security toolkits are a genre of online guide that seek to instruct users on how to protect their security online. These toolkits often take the form of tutorials or step-by-step guides, though some break in form appearing instead as zines or even as "app stores" (similar to those found on smartphone platforms). We look to security toolkits because they promote different notions and conceptions of what and for whom security is sought.

#### 2.2.1 Formulating Users

In investigating how these toolkits embody and claim to promote the value of security, we ask: "What design choices have been made in constructing the toolkits, and what practices do such objects advocate in the name of security?" Answers to these questions will help us better understand what security means to these groups and providers, and how both toolkits and social computing systems may provide it. They may also open up surprising opportunities for innovating on the form of security toolkits, which are themselves designed objects. Security toolkits provide us windows into the lives of those who existing security practices do not adequately protect, as well as the organizations that work to address these inadequacies.

One important strand of research related to values and design concerns how technologies conceptualize, and construct, users. In this research we seek to understand how cybersecurity toolkits construct users as insecure and, in doing so, make certain threats salient and thus amenable to defense. In adopting this perspective that technologies and their creators contribute to the construction of a user, we are in a better position to see how certain values and design decisions take on different meanings with respect to different subject positions.

Prior research in CSCW and Science & Technology Studies (STS) has articulated ways in which designers of technical artifacts configure or construct a notion of the "user," and how this configuration might be limited by the designer's own position, potentially leading to undesirable conditions for the user. STS scholar Steve Woolgar's early research on usability trials examines how the role of the user—her "character and capacity, her possible future actions"—is "structured and defined in relation to the machine" [33: 89]. Building on this work, Madeleine Akrich [3] discusses the notion that technical artifacts are "pre-inscribed" by designers who "define actors with specific tastes, competences, motives, aspirations, political prejudices, and the rest, and they assume that morality, technology, science, and economy will evolve in particular ways" [3:208]. Putting forth this notion that artifacts carry scripts, Akrich highlights the ways in which they behave as "stage directions" for the performance of using a particular technology, and draws attention to artifacts as agentive beings with the power to shift and define the situations within which they sit. While Woolgar and Akrich also discuss shifting definitions of user and scripts as technical artifacts move out of the space of design and into the world of use, our analysis of toolkits focuses on the ways their design and content reflect conceptualizations of users in relation to security, rather than how these toolkits are used in-situ or in the wild.

Recent work within HCI has interrogated the category of "user," blurring the boundary between "designer" and "user" of a technology [5]. For instance, Bardzell and Bardzell put forth the concept of the subjectivity of information, devoting careful attention to the connections between *subject position* and *subjectivity*: the role a person is given within a particular context and the lived experience and agency of that person as the situation unfolds [4: 134]. The authors argue there is no single, universal "user," but that technological designs are embedded with

particular subject positions; users co-create and negotiate multiple subjectivities through their use of the technology. Hardy and Lindtner draw on this work and connect to broader discourses on sexuality and identity, in order to explore the multiple subjectivities negotiated by users of location-based dating applications for gay, bisexual, queer men [15]. In doing so, they argue that these technologies not only construct a particular type of user, but also construct the forms of sexuality available to them through the app—forms that reflect the apps' founders and designers, which shape the lived experiences of users. In connecting this work to a values-based approach to security, we argue that security as a social value: that its conceptualization, its supporting practices, who is seen as a salient object or subject of security, vary among the different subject positions and subjectivities that security toolkits present.

In this paper, we draw on these complementary strands of research to analyze cybersecurity toolkits, and to surface the values and politics embedded within their design. Specifically, we seek to understand how security toolkits construct insecure users, and in so doing, inscribe rituals of self-protection. In other words, we seek to surface what notions of (in)security are embedded within each toolkit (by the designers and cultural contexts that produce them) to understand how insecure users are configured to protect themselves.

## 3 BACKGROUND: SECURITY TOOLKITS

Security toolkits are a genre of online guide that seek to instruct users on how to protect their security online. These often take the form of tutorials or step-by-step guides, though some break from this form by appearing as zines or "app stores." Many exist to ensure security, either against the threat of surveillance or threats to personal safety such as doxxing (the practice of publishing a person's personal information without consent, a common tactic among online trolls [8]). Often, toolkits seek an audience of "marginalized" or "vulnerable" groups, who may be especially motivated or forced to protect themselves against specific threats faced by their particular communities, such as hate speech or doxxing. Next, we provide an overview of what toolkits are and how they are organized.

### 3.1 What are security toolkits?

Broadly, our criteria for security toolkits are (1) collections of tools and actions, (2) actionable and usable for individuals and groups, which are (3) offered as solutions or other ways of addressing immediate user needs related to cybersecurity. We use the term security toolkit to refer to a loose genre of artifacts that provide a variety of tools that members of the public can use to help them perform particular security practices. The original inspiration for this study came from our observation of many different toolkits curated and disseminated by non-profit, grassroots, and activist organizations. While our definition of security toolkits is quite inclusive, the core set of objects analyzed in this paper is more restrictive. The set of toolkits we selected for close analysis was the result of an iterative process of definition, collection, and analysis that we describe further in the Methods section.

For the project at hand, we examined two overlapping forms of the security toolkit. The first type sought to address nonspecific populations, or in other words, "everyone." For example, the U.S. Department of Homeland Security's *Stop.Think.Connect* toolkit [40] and the Electronic Frontier's *Surveillance Self-Defense* toolkit [42] seeks to offer recommendations for anyone who is concerned about their digital security. The second set of toolkits express support for people with a distrust of or conflict with institutions such as governments, service providers, and device manufacturers. For example, *SecureDrop* [51] is a toolkit for political dissidents or whistleblowers

to share documents with media organizations, brokering a connection in the presence of untrusted governments or intermediaries.

Many toolkits proffer a predefined set of actions one might take to ensure one's online security. Common examples include webpages and components titled "create and maintain strong passwords," "enable two-factor authentication," and "threat modeling." Another common form taken is software tools—almost always free to download—that users may acquire, configure, and use. These represent concrete, stand-alone tools for people to use and, potentially, repurpose. The *Tor Browser* [60], for example, offers a sense of anonymity in the presence of untrusted web companies and internet service providers (ISPs) through their software toolkit providing anonymous web browsing (built on the Tor onion-routing network). Other examples of software tools discussed within toolkits include password managers, the encrypted messaging application *Signal*, virtual private networks (VPNs), particular browser plugins, utilities for two-factor authentication (2FA), and smart phone settings that allow users to opt-out of interest-based ads.

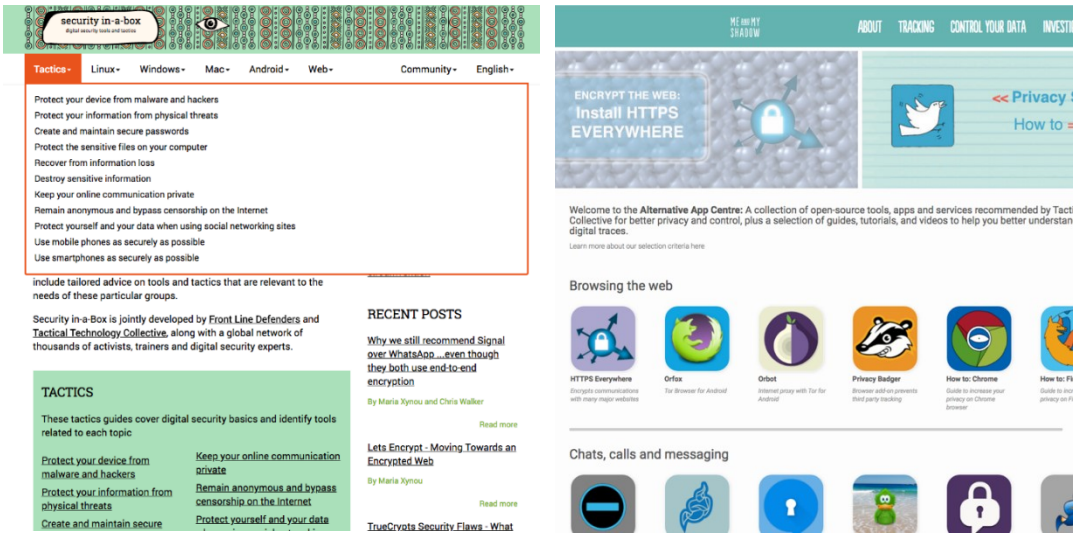


Fig 1. (Left) Security In-A-Box toolkit by Tactical Tech collective provides a set of tactics and actions one might take [45]; (Right) Alternative App Centre page from the Me and My Shadow toolkit suggests secure mobile apps for users to download, taking the format of an alternative app store [46]

Some toolkits act as services, where users interface substantially with human providers. Examples include Access Now's *Digital Security Helpline* for human rights defenders [43], *SecureDrop*'s anonymous file transfer service used by journalistic organizations [51], or *Simply Secure*'s educational service offerings to user experience professionals [52]. Other toolkits include tutorials that educate people on cybersecurity and surveillance concepts. In some cases toolkits present original content, while many more link to third-party materials.


Fig. 2. (Left) Digital Security Helpline for human rights defenders by Access Now! provides a service for individuals and organizations who are at risk online [43]; (Right) Explanation and tips for phishing attacks from the U.S. Department of Homeland Security's Stop.Think.Connect toolkit for a general population [40].

While most toolkits feature software tools or services, some also recommend ways of modifying or acquiring alternative computer hardware or electronic devices. The Electronic Frontier Foundation, for instance, discusses the use of burner phones ("A phone that is not connected to your identity") and configuring a "secure machine" [42]. Imminent Threat Solutions recommends shielding your credit card information and using a "USB condom" (a protective hardware shield)

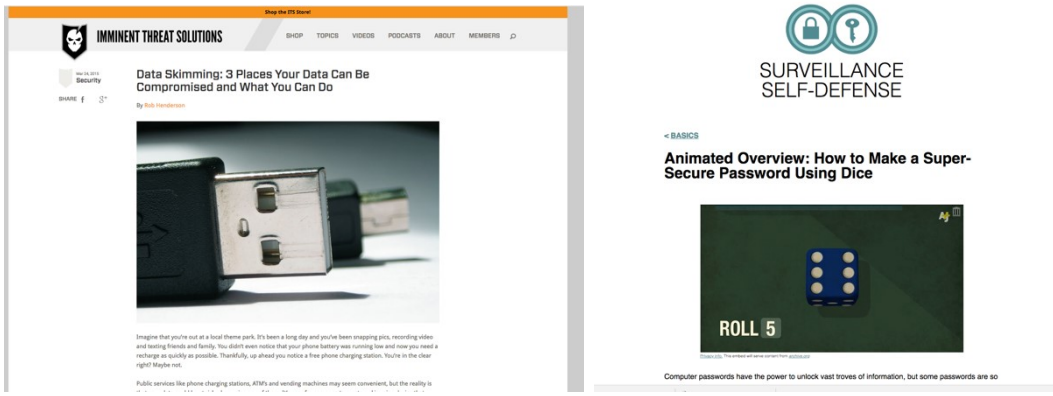


Fig. 3. (Left) Recommendations for securely using physical devices by Immanent Threat Solutions [66]. (Right). Instructional video demonstrating "How to Make a Super-Secure Password Using Dice" from the Electronic Frontier Foundation's Surveillance Self-Defense toolkit provides a technique for password creation that readers can learn and use [42].

to prevent malicious data exchange while charging devices [66]. In a few cases, we found examples of toolkits that recommend or discuss non-digital technology tools or interventions. These include using tape or stickers to cover webcams, writing down passwords, and keeping a physical safe to store sensitive documents and digital backups.

A unique class of toolkits are offense-based, as opposed to defense-based. A key example is the *Low-Orbit Ion Cannon* [44], a tool for stress testing networks by conducting DoS (denial of service) attacks to demonstrate potential security vulnerabilities. Another is the practice of doxxing or outing members of online hate groups. These controversial practices appear to stem

from a belief that offensive measures can help defend against future attacks. A number of provocative and activist tools also illustrate speculative and experimental techniques of offense-based cybersecurity. For example, *Ad Nauseum*[1] is a browser extension that quietly clicks on every ad within the browser page in order to obfuscate the detection of personal preferences and patterns. Adopting counter-surveillance, examples such as Adam Harvey's CV Dazzle[2] face camouflage for digital surveillance or NeuroSpeculative AfroFeminism collective's *HyperFace* anti-surveillance scarf exemplify tactics of resistance that also bring visibility to surveillance and data collection practices, and the need for tools to subvert and resist these practices.

The existence of this broad range of cybersecurity tools complicates the frame of security as being either about prevention or response to an attack. Instead, they suggest radical modes of preemption and counterattack as methods of achieving security. In the following section, we detail our process of toolkit selection and analysis.

## 3 METHODS

To produce our corpus of toolkits, we searched online and solicited recommendations among colleagues and associates during early 2018. Given our interest in security as a value from different subject positions, we primarily focused on searching for toolkits aimed to serve user groups that may have higher or different types of risks or have been historically marginalized. We only included toolkits in our corpus that discussed digital security for end-users and we limited our search to English-language toolkits due to the language proficiency of authors. However, several toolkits are available in multiple languages, particularly those designed for human rights defenders. We only considered toolkits that were accessible via the Internet, and thus excluded most toolkits only accessible from within an organization, such as internal cybersecurity training materials.

The initial set of toolkits that inspired this study consist of highly curated collections, often by organizations that appear well funded, and typically with original content in the form of tutorials, instructional videos, and marketing and branding materials. The organizations that create these toolkits are typically non-profit activist organizations. Examples include the Electronic Frontier Foundations Surveillance *Self-Defense* toolkit [42], Tactical Tech's *Security in a Box* toolkit [45], and Digital Defenders Partnership's *Digital First Aid Kit* [48]. However, we then moved to expand our collection of toolkits to include specialized tools and services such as *SecureDrop* [51], corporate and governmental toolkits such as Facebook's *Security Checkup* [37] and the U.S. Department of Homeland Security's *Stop.Think.Connect* toolkit [40], as well as blogs and articles by individuals outlining checklists and tutorials, such as a medium post by Middle School teacher Candice Williams presenting *A 70-Day Web Security Action Plan for Artists and Activists Under Siege* [68]. As we collected toolkits, we shared notes on who created them, who we thought the intended or anticipated audience or users of the toolkits were, and other information about the toolkits that stood out to us. We recorded this information during our individual observations and discussed it at periodic group meetings. To sample for diversity in our corpus of toolkits, we began by looking for toolkits made by different authors, including activist groups, technology advocacy organizations, and government organizations. Since many toolkits link to or aggregate other toolkits, we allowed our sample to "snowball" until we could not find any more samples from different types of groups or that speak to different types of audiences. By the end of our initial search, we produced a set of approximately 30 toolkits for analysis.

[1] See https://adnauseam.io/
[2] See https://cvdazzle.com/

To broaden the diversity of the toolkits in our corpus, we then actively sought out toolkits that might highlight positional vulnerabilities for groups antagonistic or hostile to the different subject positions and user groups represented within the initial set of toolkits references. We found a few examples of toolkits that try to help provide security to those who want to explicitly practice online hate speech, commit cyberharassment or bullying, or have an antagonistic point of view toward the U.S. federal government. This added an additional set of approximately 10 toolkits to our corpus for analysis. Recognizing that the subject positions of the creators and intended users of these toolkits are likely very different than those from the toolkits in our initial corpus, we did not seek these out to put all toolkits on an equal playing field, but rather sought out these toolkits to understand whether they suggest a different orientation to or conception of security. Since the number of potential toolkits we could collect is enormous, after collecting our core set of toolkits, additional toolkit collection was guided predominantly by the goal of seeking diversity in form, function, audience, and creator. After collecting 41 toolkits, our group determined we had a sufficiently diverse sample for our goals.

During the process we also decided to exclude toolkits we interpreted as highly artistic and experimental, including the aforementioned face camouflaging *CV Dazzle* tutorial by artist Adam Harvey. This decision was based on our interpretation of such tools as both intended for and used primarily as artistic provocations and awareness-raising mechanisms rather than pragmatic tools for use by people facing security threats. While the exclusion of such toolkits from our final group of 41 means we did not analyze them closely for this paper, these and other toolkits that ultimately fell outside of our core definition of cybersecurity toolkit nonetheless informed our thinking about toolkits and the resulting concepts discussed in this paper. We believe that analyzing them more closely in the future would produce additional insight into security broadly.

We then conducted several rounds of analysis employing an interpretive and iterative process. In a first round, all authors examined the toolkits to understand how security was being framed, noting what practical uses, features, or suggestions the toolkits suggested; the broader roles the toolkits suggested that they play socially, politically, and organizationally; and how the toolkits conceptualized security. Each author recorded these observations individually by writing memos and drawing diagrams. These memos and diagrams were then shared and discussed at group meetings to identify emergent themes and categories. A set of initial categories emerged that were used to build toward more formal analysis.

In a second round of analysis, the authors coded the corpus of toolkits according to a set of categories that emerged from the first round of analysis. For each toolkit, we recorded the following information, along with our reasoning: for whom is the toolkit designed; whether security is presented as an achievable state or an ongoing process; and who the toolkit thinks is responsible for achieving security. Each of the toolkits were viewed and coded by two different authors. For any toolkit upon which two authors disagreed about codes, all authors reviewed the toolkit and discussed the disagreements in person. This coding process allowed us to identify themes, patterns, and tendencies with regard to these categories across the set of toolkits.

In a third round of analysis, the authors conducted a close reading of toolkits, focusing mainly on those toolkits that had coding disagreements. What emerged from this close readings was a set of nuanced discussions and distinctions that began to complicate some of the initial categories and spectrums identified, highlighting the ways in which differential vulnerabilities and differential notions of security emerge from the corpus of toolkits.

Our project group included 4 researchers with diverse expertise, with foci in the areas of cybersecurity and computer science, privacy and policy, critical and ethnographic studies of

sociotechnical systems, and user experience and design research. The entire research team shared various interests across areas of CSCW, HCI, design research, and technology studies.

## 4 FINDINGS

Our analysis is centered around several categories. First, we analyze common *genres and categories* used to organize toolkits, which includes "tactics," "tutorials," and "services." This provides a basic sense of how toolkits are structured with respect to form and content, and what basic functions they offer. From these descriptive characteristics, we then present our analysis of *touchstones* and *metaphors*—shared cultural references that motivate or contextualize particular security recommendations or pervade the design of an entire toolkit. Finally, we frame three key *design dimensions* upon which the toolkits in our sample can be assessed and categorized: agentive scale (who is responsible for security?), achievability (is security be achievable state?), and interventional stage (when are security measures to be taken?).

### 4.1 Touchstones and Metaphors

We first examine social, cultural, and symbolic aspects of cybersecurity toolkits by focusing on touchstones and metaphors. Our analysis involves tracing the ways toolkits respond to and reference broader socio-political events and narratives, looking to the textual and visual language used. These touchstones and metaphors offer insight into values, mental models, and conceptual understandings of security and surveillance which undergird the forms toolkits take and their functional offerings.

#### 4.1.1 Cultural Touchstones

Toolkits are shaped in part by cultural touchstones—narratives, discourses, events, and shared experiences in broader culture and media. Toolkits' references to these touchstones help signal particular notions of security, communicate concepts, or signal that toolkits are responding to the needs of a particular group or a particular type of harm. For instance, the term "big brother" from English author George Orwell's novel *1984* is often used in explanatory or educational materials as a way to evoke that there is a group in power that is always watching what people are doing. Sometimes it is used in reference to government- and state-based surveillance, while other times it is used to describe private companies such as online platforms and internet service providers that also have capabilities to constantly monitor users' activities. The Electronic Frontier Foundation's Surveillance Self-Defense [42] includes several references to *1984*, comparing contemporary digital surveillance with the telescreen technology featured in the novel.

Some of the toolkits we studied were created directly in response to events that shape the types of threats the toolkits try to protect against. Many toolkits either explicitly or implicitly refer to one of two geopolitical events: revelations in late 2012 by Edward Snowden about the surveillance capabilities of the U.S. government into private communications; and the results of the 2016 U.S. Election. Some toolkits were created directly in response to these events, such as the *Center for Media Justice* and the *70-Day Web Security Action Plan* being direct responses to the 2016 U.S. Election [50, 68]. Other toolkits already existed, but provided updates, blog posts, or additional information referring to these events when they happened, such as *Me and My Shadow* and *That One Privacy Site* [46,70].

Toolkits that are targeted toward specific audiences, particularly those for human rights activists, tend to highlight cultural touchstones that resonate with such groups. For instance, several toolkits aimed towards human rights activists explicitly cite the 1998 United Nations Declaration of Human Rights Defenders, including *Holistic Security* and the *Integrated Security*

*Manual* [38, 41]. The Declaration outlines the rights that human rights defenders have and the duties that states should abide by; these toolkits will often also use the U.N. term of "human rights defenders" rather than "human rights activists," signaling a shared grounding in the document, and the perspective it embeds. Some touchstones are more local; *Security in a Box* points to an incident from 2001 in which 52 men were arrested for "debauchery" at a gay nightclub, an event described as "the turning point for LGBT rights" in North Africa [45].

A number of toolkits use individual experiences as touchstones, particularly toolkits that focus on preventing or addressing online harassment. Often these toolkits are created by people who themselves have been the target of online harassment, doxxing, or cyber mob harassment, such as *Crash Override, Equality Labs Digital Security 101,* and the *Speak Up and Stay Safe(r) Guide* [47, 49, 55]. The conceptualization of security in these toolkits goes beyond technical digital security to include emotional and social aspects. In these cases, security is a way to empower people who have been, are, or could potentially be the targets of online harassment. For instance, the authors of the *Speak Up and Stay Safe(r) Guide* state: "We created this document because we wanted to share what we have learned through years of being targeted by cyber mobs. We know how intimidating, scary, and overwhelming online harassment can be and we hope this document can help to empower readers to make informed safety and security decisions that are right for them" [55]. Drawing on offline practices of responding to harassment, several explicitly state that it is "not your fault" if you are targeted and discuss resources for social and emotional health in parallel with digital security techniques.

From this set of cultural touchstones, we can begin to trace how these toolkits respond to and leverage broader socio-political events, discourses, and stories.

#### 4.1.2 Metaphors

Whereas touchstones describe shared reference points, *metaphors* evoke different approaches to, or perspectives on, cybersecurity—for instance, who and what should be secured, how security should be enacted, and who is responsible for enacting it. The metaphors and tropes we uncovered in our analysis range in association from medicine and public health to self-defense and tactical resistance.

Some toolkits such as *The Speak Up & Stay Safe(r) Guide* discuss security practices through associations with preventative care (here called "prevention measures") [55], or medical action taken to prevent rather than treat disease. In making this association, designers of the toolkit implicitly suggest one who takes preemptive security action is making responsible moves to avoid future security incident. Other toolkits use the concept of first-aid as a way to indicate their role as responders to incidents that have happened or are currently underway. For instance, the Access Now D*igital Security Helpline* provides "rapid-response emergency assistance" through 24/7 telephone or chat support [43] (in a similar fashion to emergency response call systems like 9-1-1 in the US or suicide hotlines). The Digital Defenders Partnership calls their set of diagnostic procedures the *Digital First Aid Kit*, aimed at helping "digital first responders" offer support to those experiencing "digital emergencies" [48]. Similarly, the *70-Day Web Security Action Plan* [68] references cabin depressurization airplane emergency procedures—putting on one's own oxygen mask before assisting others—in suggesting that individuals should first care for their own security practices before helping those around them.

Other toolkits use educational metaphors such as "tutorial," "courses," or "primer" to suggest their aims are to teach people about aspects of security, such as explaining technical underpinnings of systems or aspects of threats, risks, and self-defense mechanisms. Similarly, other toolkits discuss "digital training," noting skills or practices will be imparted through the

course of the interaction (rather than the presentation of static information). Relatedly, toolkits such as *Hackblossom DIY Guide* and *Chayn Do It Yourself Online Safety* suggest a scrappy taking back of control over one's digital life, using terms popularized among alternative art and punk music scenes to define their security practices [58, 64]. While most of these toolkits focus on the education or action of technology end users, a few such as *Simply Secure* aim to instruct those creating the digital systems in question—namely, technology designers [52]. Some such as the Electronic Frontier Foundation's toolkit [42] also propose that they are a "starting point" for developing security practices, acknowledging limitations of the resources they offer and that over time, without regular upkeep, the contents of the kit may not contain the most up-to-date information.

A range of "self-defense" or "tactical" actions occupy a number of toolkits supporting individuals organizing for social change. *Holistic Security Guide*, for instance, describes their approach to security as being centered on "holistic [approaches] and well-being as subversive and political" [41]. Rather than focus on particular, named adversaries, these kits identify instead those presumed to have shared a set of knowledge or experiences. For example, *Advocacy Assembly* states that its resources are "designed for women, people of color, trans and genderqueer people, and everyone else whose existing oppressions are made worse by digital violence" [54]. The *Resisting Doxing* guide simply states that "marginalized people are targets online" [56]. In both cases, particular adversaries are substituted for the status of the people under threat. These observations surface the ways in which adversaries are framed, what gaps and absences exist in the way they are portrayed as threats, and how these threats are connected to their anticipated online behavior.

Elsewhere, security is discussed as an ongoing practice, aligned with "hygiene" which one might perform on a daily basis or as periodic "checkup." The notion of hygiene implies a kind of ongoing commitment, and an orientation toward a particular vision of cleanliness and upkeep. It draws associations with sanitation and disease prevention. Meanwhile, the trope of the checkup—used to describe security instruments across prominent firms such as Google and Facebook [37]—communicates the preventative function or anticipatory measure of the tools. Rather than a step that might be integrated in the ordinary, day-to-day interaction procedure, the checkup is something set apart, an act one volunteers to participate in based on a particular interest or concern. It sits distinct from the more responsive tools that guide one through an already underway security breach or attack. It instead suggests a kind of carefulness or safeguard on the part of the individual consumer or institutional actor, perhaps akin to a yearly examination at doctor's office or an inspection that might check for compliance at a commercial establishment. Here, precaution and forethought are rewarded through the refinement and customization of one's individual system level preferences (restricted, of course, by the controls offered by the firm).

### 4.2 Design Dimensions of Toolkits

Through our analysis, we arrived at three design dimensions evident in the toolkits we studied. We use the term "design" broadly to consider the content of the artifact, including tactics and rhetoric. The dimensions we surface reflect design decisions and highlight critical differences in the ways toolkits frame the process of security. These dimensions do not only represent different security practices, but also different notions of security that apply differentially across diverse populations with heterogeneous needs. These dimensions are critical in motivating our notion of differential vulnerabilities, which we introduce in the discussion.

| Design dimension | Question | Scale |
|---|---|---|
| **Agentive scale** | Who is meant to perform security? | Individual user ←→ Group |
| **Achievability** | How achievable is security portrayed to be? | Achievable ←→ Ongoing |
| **Interventional stage** | At what point is security envisioned to be performed? | Before attacks ←→ After attacks |

Table 1. Design dimensions. Scales on which we may evaluate the rhetorical position of security toolkits.

#### 4.2.1 Agentive Scale

The first dimension we examine is on *agentive scale*: Who is imagined as being capable of, and responsible for, achieving security? Within the toolkits we analyzed, most focused on technical measures individuals might take to protect their own security. For instance, one might install and use specific programs or apps such as *Tor* for web browsing, *Signal* for encrypted messaging, or virtual private networks (VPNs). Other techniques might involve changing application settings, encrypting devices' hard drives, or enabling two-factor authentication procedures. Still others suggest approaches aimed at limiting corporate data collection, such as using alternative search engines (e.g. *Duck Duck Go*) or configuring particular social media settings (i.e., disabling geotagging on shared posts).

Some toolkits also highlight the importance of social and emotional dimensions of maintaining security. For instance, the *Speak Up & Stay Safe(r)* toolkit pairs a range of technical measures with a section on "people-focused strategies" [55]. Here, the toolkit suggests that if targeted online, it is important for one to acknowledge the need for forms of self-care and to potentially seek formal mental health resources. The toolkit also begins to suggest group or community-oriented responses, offering recommendations on the ways individuals who have been targeted online might reach out to friends, family members, colleagues and employers. Notably, though, within this "people-focused" approach, the individual holds the responsibility to connect and communicate with others during times of disquiet, rather than the toolkit positioning the state of security or secureness as a communal endeavor (by notifying a trusted contact in times of threat, for instance).

Toward the communal end of the scale, Tactical Tech's *Holistic Security Manual* builds upon this recognition of the social and emotional dimensions of security to expand the range of responsibility from the individual to the broader community [41]. For example, the toolkit recommends creating affinity groups—or a small collective who together prepare for, participate in, and travel to and from direct actions (e.g. protests, sit-ins) to both ensure immediate physical safety, but also to foster forms of collective responsibility and care. "It can be useful to coordinate with a group of friends of colleagues in order to act together and take care of one another," the toolkit notes (in Section 4.2) [ibid]. Within the toolkit, discussion of the impacts of trauma, stress, and fatigue sit alongside (with equal weight) individual, technological responses to security threats.

#### 4.2.2 Achievability

The second dimension is *achievability*, or to what extent security can be accomplished or realized. At one end of this spectrum is *security as achievable*: the notion that, if a user follows a particular set of defined steps, they will reach a secure state. This framing of security is clear in toolkits that suggest using particular tools or applications, or other technical measures that might be undertaken. For instance, the *Me and My Shadow Alternative App Center* provides a set of

alternative web browsers, messaging apps, search engines, and other "alternative" versions of common services of applications that either encrypt or do not track end user data [46]. This suggests that if people are able to download and use these applications, then they will have realized security. Other toolkits imply the achievability of security by providing step-by-step instructions to change system settings or install secure tools and applications. These often take the form of guides, checklists, or tip sheets.

At the other end of the achievability spectrum is *security as an ongoing process*. Although fewer toolkits that we reviewed took this perspective, several provided indications that security might be a routine practice, rather than a sort of conclusive state one might achieve. Toward this end, toolkits within this genre provided a set of practices and tactics that addressed a cyclical understanding of security. *Holistic Security*, for instance, acutely embodies this perspective, pairing "psycho-social well-being and organizational security processes" [41] to form an approach that is long-ranging and differentially applied based on aspects of one's identity (e.g. one's personal history alongside culturally ascribed attributes of gender, race, and nationality, socioeconomic status). This awareness of the contingency of security is expressed in the guide's description as a "strategy manual," perhaps creating links to Certeau's [7] notion of "strategies" as they relate to large institutional structures and how they make the space in which citizens/consumers operate. Yet, distinct from Certeau, the actors in this case are collective in nature (rather than individual) and seem to take up certain creative acts of resistance that might typically be associated with "tactics." Here, security is an "evolving, cyclical process and should be regularly revisited as part of our ongoing strategic planning" [41].

In between these two ends of the achievability spectrum, we identified a number of toolkits that occupy a midrange where security is framed as something to be managed periodically. This category includes those that frame security as "checkups," such as tools built into social media sites (e.g. Facebook) that encourage users to review their security settings from time to time. While an individual checkup might suggest that a particular configuration of settings allows security to be achievable for a period, the notion that one needs to review and reassess these settings over time suggests a longer-term, process-oriented approach. Some toolkits also try to broaden users' understanding and capacity to take security measures. These go beyond step-by-step instructions of how to install applications or change settings. For instance, the *Surveillance Self Defense* toolkit contains a "Further Learning" section, with materials explaining what public key cryptography is and how it works [42].

Notably, not all toolkits sit at single point on the achievability spectrum. Some toolkits we reviewed assume security as a process, but this perspective is not always reflected in the steps they provide or prescribe. For instance, *Surveillance Self Defense* describes security as something that ought to be incorporated into one's daily routine in its introduction, stating that "there is no perfect security—there's always a trade-off" [42]. However, the toolkit itself is comprised of a series of how-to guides and off-the-shelf solutions to solve particular security issues, giving the sense that if one were to complete each item (developed by "experts") one might achieve security (we further discuss such dissonances in Section 5.2).

#### 4.2.3 Interventional Stage

Finally, interventional stage is the third dimension we surfaced through our analysis. This dimension is concerned with the temporal relationship between an intervention, such as a tool or toolkit, and the threat of attack against which it seeks to protect. On one end of this spectrum are *preventative measures*, which involve risk modeling or forestalling the likelihood of future threats (but do not help in mitigating damage that has already occurred from an attack). Only a few of the toolkits we found fell into this category. On the other end of this spectrum, *provoked responses*

involve mitigating attacks that have already occurred (but do not focus on managing risks of future attacks). For example, the *Digital Security Helpline* offers real-time assistance to human rights defenders in the form of a "crisis hotline," a phone number one might call to speak with an expert about security measures one might take in the case of an emergency [43].

Most of the toolkits in our analysis sit in a middle space, taking interactional measures, which seek to protect users against threats that are ongoing. The toolkits in our sample advise users on both how to mitigate damage they may have already encountered (e.g., removing listings on "people search engines'" commonly used by doxxers), as well as how to manage future risks (e.g. encrypting files in the case of seizure or leaks). Many guides may fill both of these roles in a single step. For example, the EFF's *Surveillance Self Defense* [42] recommends users install a password manager and change their existing login credentials, to both minimize the risk of future breaches and the harm of leaks that may have already occurred. In the following section, we use these dimensions to draw out discussion on how the toolkits conceptualize security in multiple ways through the notion of differential vulnerabilities, and provide insights informing broader discourses of security.

## 5 DISCUSSION AND IMPLICATIONS

As technologies, the toolkits we studied illustrate the design and marketing of actions people can take to protect their security online. These toolkits also serve as embodiments of ideas, values, and the framing of problems and solutions pertaining to digital security; they reveal high-level insights concerning the state of security tools, discourse, and practice.

This paper does not offer a solution to security, nor are we critiquing toolkits for failing to offer "complete" security (indeed, the heterogeneity in the corpus of toolkits analyzed highlight that it is intrinsically unclear what constitutes a security solution). Instead, we find that toolkits present a way of *doing* security, an enactment that maps to Dourish and Anderson's model of practical action [11]. Our empirical work builds on this model with the observation that these enactments secure different bodies and institutions in different ways, offering a glimpse at the multiplicitous enactments of security. These diverse enactments underlie what we have termed *differential vulnerabilities* (discussed further below), which are addressed through the social practice of toolkit creation; a practice driven by communities, built out of necessity in an ad-hoc (and sometimes post-hoc) fashion.

In seeking to understand how the toolkits conceptualize and promote particular notions and practices of security as a worthy social value from the perspective of different subject positions, we were particularly interested in how these toolkits configured users as insecure. In most of the toolkits we analyzed, security is framed as a user's personal responsibility. This idea embeds neoliberal assumptions about technology use and the safety risks it entails as matter of individual choice. This approach contrasts with a minority of toolkits we analyzed that frame security as communal responsibility, a socially situated practice in which community members provide technical and emotional support to achieve a collective notion of being secure. Although we gesture toward possibilities within this design space below, our findings endorse future work on the political ramifications of security's agentive scale. What sorts of threats are made (in)visible as such through these agentive scales? Work on this question will help inform the reasons for, and consequences of, design decisions in toolkits broadly.

Similarly, our work surfaces a diversity of adversaries that toolkits define, which includes not only "criminals" or "bad actors" but also corporations, governments, and other service providers and manufacturers. Indeed, in many cases, toolkits concretely illustrate ways in which these institutions are unwilling or unable to meet specific needs, particularly those of groups and

individuals with specific vulnerabilities such as journalists, political dissidents, and racial, ethnic, and religious minorities targeted by surveillance and online harassment.

In the remainder of this discussion, we consider the notion of differential vulnerabilities that we have developed through our analysis of security toolkits. We use this notion to outline novel possibilities in the design space of security toolkits.

### 5.1 Differential Vulnerabilities and Trust

Our work surfaced the heterogeneity and diversity, not only of the forms of security toolkits, but also of the types of threats that they describe and seek protection against. Here, we return to one of our initial questions: how do toolkits construct users as vulnerable? The diversity of inscribed rituals of self-protection highlights that users are not only constructed as vulnerable, but that different toolkits construct users as differently vulnerable from one another.

This observation motivates one of our key contributions, the concept of *differential vulnerabilities*. The notion of differential vulnerabilities recognizes that different populations and individuals have different types and degrees of digital security vulnerabilities and may be targeted in different ways. This stands in contrast to dominant technical security discourses that frame security as an objective or universal value, and the "insecure user" as an objective state. Like recent work reframing values as practices and processes rather than static objective goals [16, 21], the concept of differential vulnerabilities shifts thinking about security and its related phenomena (such as vulnerability, risk, or trust) from an objective measure to a marker of relational positions that are maintained, contingent, and may change over time. This shift is also influenced by feminist, queer, and race studies perspectives on vulnerability. Rather than describing vulnerability as "an inherent quality or characteristic of some bodies," feminist theorist Sara Ahmed instead suggests that "vulnerability involves a particular kind of bodily relation to the world," which is experienced differently by different bodies [2:68-69]. Critical race studies scholar Zeus Leonardo, in discussing dominance, power, and privilege, distinguishes between "dominance" as a state of being, and "domination" as a process which makes possible the social condition of dominance [22]. In a similar move, we use "differential vulnerabilities" to pay attention to processes of creating and maintaining relational positions of being vulnerable. This shift challenges the notion of "vulnerable populations" as a pre-existing category, raising questions instead concerning "*who is vulnerable to what?*", as well as, "*who applies the label of vulnerable?*" For values in design researchers investigating security, the lens of differential vulnerabilities can offer focus on processes of how vulnerable positionalities are made and maintained. While we investigate how toolkits create and maintain these positionalities, future work might look to the ways other practices and processes of security influence such relations.

Through our analysis, we found a great deal of evidence for positional vulnerabilities "on the ground" as manifested in the design, development, marketing, and advocacy of various toolkits. For example, based on variance in the agentive scale of toolkit design, we found toolkits focused on the security needs of journalists, activists and organizers of color, trans and genderqueer people, political dissidents and human rights activists, police and law enforcement professionals, and even communities of trolls and hate groups whose actions are often the subject of legal action, legislation, and many of the aforementioned toolkits. Looking at the achievability and interventional stage scales, we also found that toolkits created by non-profit or activist groups focused much more explicitly and effectively on forms of differential vulnerabilities than comparable corporate and government tools and toolkits, which tended to treat all users as similar. For example, Facebook's *Security Checkup* appears to offer the same checklist for

everyone, disregarding differences such as one's likelihood of being a target of surveillance or cyberattack.

This concept also casts new light on the notion of "vulnerable populations," a term often used in academic literature, journalism, grant solicitations, and conference and journal calls. While it is indeed important to focus research, design, and advocacy work on diverse and marginalized groups and individuals, there are also some problems with broadly characterizing people as vulnerable populations. This term may stigmatize and disempower those labeled as vulnerable by portraying people as lacking strength, resilience, and ability, as well as ignore people who may be at risk but not considered a "vulnerable" population [30]. The language of vulnerable populations also constructs a power relation in which researchers, engineers, or policymakers assume the role of protector, which can work to reaffirm inequitable power relations. In our analysis, we only encountered one toolkit that explicitly referred to "vulnerable groups," suggesting that this term is not favored or used by members or organizations working closely with so-called vulnerable populations.

Following these observations, we propose that the concept of differential vulnerabilities provides an alternative, one that avoids some of the pitfalls associated with "vulnerable populations." More importantly, though, we believe this term can be useful in allowing academics, security experts, activists, and others to discuss specific vulnerabilities in relation to classes such as race, social class, religion, gender, and sexuality, as well as more specific and personal attributes, such as the positional vulnerability of transgender youth who are repeated targets of cyber bullying and harassment. By highlighting differences of experience between groups, the term allows us to speak more directly (and concretely) about *everyone's* vulnerabilities, including those not ordinarily considered as "vulnerable populations" (e.g., lawyers and parents with teenage children). There are parallels here to inclusive design and discourses in disabilities studies within computing research, such as recognizing situational disabilities and the differing capabilities of all people. The concept of differential vulnerabilities can thus facilitate discussions about the specific conditions of a person or group as well as the specific vulnerabilities of *all* persons and groups. In contrast, the term vulnerable population can both flatten differences within a group while amplifying differences in relation to an implied normal, safe, and secure dominant group.

The concept of differential vulnerability leads to a second related notion, that of *differential trust*. In practice, it is unclear who trusts whom with what. The technologies and institutions that will protect the interests of users depend highly upon which users need to be protected, and their standing within particular social groups and contexts. We saw evidence for differential trust in many instances of non-overlapping resources within the toolkits we studied, emerging from looking at the agentive and achievability scales and thinking about *from what* they aim to provide security. For example, many counter-surveillance toolkits recommend using Tor and Signal for anonymous web-browsing and messaging. However, the U.S. Department of Homeland Security's *Stop.Think.Connec*t toolkit and Facebook's *Security Checkup* do not recommend Tor or Signal. One explanation for this is that these specific tools conflict with the business models and goals of these organizations.

Together, differential vulnerabilities and trust present two key aspects to consider when studying cybersecurity issues or creating tools to combat threats. We also observe a need within security discourses to discuss different types of vulnerabilities that hinge on positional and contextual factors, and to recognize the differing and often competing views of who can be trusted based on conflicting values and interests.

### 5.2 Rhetorical Misalignments

When analyzing the toolkits' design dimensions, we found some of the rhetorical statements within cybersecurity toolkits do not neatly match the types of activities and procedures that they discuss. Many of these misalignments surfaced while we were trying to code toolkits along our three analytical design dimensions (agentive scale, achievability, and interventional stage). When trying to resolve areas where two separate researchers disagreed on how to code a particular toolkit, we realized that the toolkits themselves were not wholly consistent, sometimes rhetorically focusing on one aspect (such as describing security as a communal responsibility) but suggesting actions that focus on an different facet of security (such as suggesting individual actions). This can lead to obscuring potential barriers, limitations, or situational aspects of cybersecurity. While it is not altogether surprising that such rhetorical misalignments exist, they do illuminate tensions occurring within security toolkits and different approaches to framing and resolving security needs. For example, the EFF's *Surveillance Self-Defense* toolkit's "Choosing your tools" page states, "security is a process, not a purchase." [42] This suggests that security is an ongoing practice. However, several of the guides within this toolkit fall into the category of "tutorials" and "how-to" guides — with concrete directives to install the app Signal or enable Two-Factor Authentication — and appear to frame security as achievable. Similarly, the *Digital First Aid Kit*'s introduction declares, "everyone has the ability to take preventative measures to avoid emergencies and responsive steps when they are in trouble" [48]. However, the toolkit's guides focus on measures for individuals to take and there is little information within the toolkit about communal or social practices. In this case, it may be that toolkits creators *aspire* to support communal and social security practices, but in practice it is individual steps and measures that are much more accessible and commonplace.

Rather than evidencing deep flaws, in our view these rhetorical misalignments instead reflect inherent contestation due to differential vulnerabilities and trust, along with potential gaps between theoretical conceptions of security and the pragmatic realities of doing security "on the ground." There will always exist tradeoffs and pressures in people's security relationships, needs, abilities, and vulnerabilities, as well as differences in the dimensions and capabilities of security resources, and toolkits may use rhetorical misalignments (knowingly or not) to reveal or conceal these tensions. Further attending to rhetorical misalignments may work to reveal different pragmatic tactics and strategies, and ultimately lead to the design of more cohesive security toolkits. Locating such rhetorical misalignments can also reveal opportunities or shortcomings, such as an aspirational rather than actual capacity for many toolkits to support communal and social security practices.

### 5.3 Over- and Under-Represented Design Dimensions

Through our analysis of toolkits in terms of agentive scale, achievability, and interventional stage, we drew out patterns and tendencies across and within toolkits. Here we reflect on some of the trends we uncovered. In some cases, these suggest needs and opportunities for tools that can complement or serve as alternatives to the functional tendencies of core toolkits. In other cases, the existence of specialized toolkits suggests ways to revise and improve tools embedded within larger platforms and services, such as Facebook or Google. And by looking at outlier and extreme toolkits, we point to some more radical alternatives to consider in the design and development of future toolkits for addressing a greater array of differential vulnerabilities and trusts.

#### 5.3.1 Designing Collective and Community Toolkits.

Most of the toolkits we encountered are designed and directed toward an individual user. On the one hand, this could be expected given that individual user has emerged as a key construct guiding the design of interactive computing technologies—even those designed to supported social and cooperative practices. But on the other hand, it is surprising to see so many toolkits prioritize the individual user given the values of community and collective action that factor so prominently into the framing of many of those we reviewed. As we discussed in the previous section, many toolkits evidence a tension between individual agency and responsibility, and collective and community values and aspirations.

The preponderance of individualizing tools, tips, and tutorials combined with the design of toolkits around particular communities with differential vulnerabilities indicates to us a need and opportunity for designer, developers, marketers, and researchers to continue to explore cybersecurity tools built around more collective, communal, and organizational models and goals. For example, rather than assuming isolated individuals are responsible for managing every facet of their own security, toolkits could be designed as services or as organizational roles for those who need security but do not work within organizations with the resources to hire a dedicated cybersecurity team, offer training sessions, or purchase the most advanced tools and technologies. Toolkits might also expand beyond the individual to consider cases such as individuals or groups serving as cybersecurity experts or managers within a community of friends, family, or coworkers.

Whether or not the implementation of such suggestions would ultimately prove effective or desirable, our analysis suggests that the developers and advocates of security toolkits should more strongly consider the curious privileging of individual choices and responsibilities given the extent to which politics and practices of community and cooperation factor so prominently into the goals and values of the organizations and groups they aim to serve. Experimenting with communal, collective, and cooperative security tools—perhaps taking inspiration from some of the toolkits we reviewed such as the Holistic Security's tactics of team and peer threat responses—appears to be a ripe design space awaiting further exploration and research.

### 5.3.2 Mainstream Tools for Differential Vulnerabilities

Finally, our research revealed a distinction between toolkits developed by smaller non-profit organizations and those developed by large mainstream organizations including governmental organizations, corporate manufacturers, and service providers. For instance, we found few examples of government and corporate sponsored toolkits that address specific differential vulnerabilities, such as those of journalists, political activists, or LGBTQ communities. Instead, it was smaller non-profits and grassroots organizations that offered these types of resources. However, the funding mechanisms for these toolkits were often unclear; it is possible that support came from governmental granting agencies or corporate sponsors. In future work, tracing the fiscal sources of these toolkits could provide important additional insight into the network of interests supporting the development and distribution of different security toolkits.

But whatever the case, we see clear opportunities for service providers and manufacturers to more explicitly address and accommodate differential vulnerabilities through the specific tools and interface options they offer their customers and users. For example, within the US Department of Homeland Security's *Stop.Think.Connect* toolkit we found no mention of the differential vulnerabilities of activists, journalists, whistleblowers, LGBTQ communities, human rights defenders, or ethnic and racial minorities targeted by surveillance. Similarly, within Facebook's Security Checkup we found no mention of hate speech or doxxing.

We also noted absences within governmental and corporate toolkits that highlight the complexities of addressing differential trusts. For example, the US Department of Homeland Security's *Stop.Think.Connect* toolkit does not recommend using end to end encrypted messaging tools like Signal, or anonymous web browsing tools like *Tor*. Facebook and Google do not recommend using an adblocker as a way to reduce the risk of clicking on a phishing attack or limiting the types of data you share online that could fall into the hands of an attacker in the event of a security breach. Yet many other toolkits did recommend taking these measures.

These absences are not unexpected given that they appear antagonistic to the goals and business models of major institutions (e.g. surveillance of citizens, collection of user data, participation on an ad-driven platform), and yet these tools are recommended by many activist and non-profit toolkits. This finding suggests opportunities for governments and corporations to explore ways to regain trust by offering a greater diversity and selection of security tools, even if such resources may work against their immediate business or governance goals. This finding also underscores the need to continue to support and develop toolkits by smaller organizations and non-profits: governments and businesses are likely not capable of fully meeting diverse needs around security when their interests too often align with the collection and handling of data that is subject to use in ways that provides security for certain groups and insecurity for others.

Our research shows how toolkits embody desires for security that dominant practices and default settings do not currently provide. Given the community-driven nature of these efforts, we propose that the creation of security toolkits can be interpreted as a form of repair [16, 20, 28], as communities take creative action to address breakdowns in security. The security toolkits we collected and analyzed provide one illuminating window into how the value of security becomes salient and materialized.

Through this frame, future work might focus on moments of security breakdown, helping to better understand how these arise from differential vulnerabilities of particular communities and how the social practice of securing-as-repair emerges in response. At the same time, this frame may help us make sense of how and why corporate toolkits, such as Facebook's *Security Checkup*, may be overly limited in their capacity to address the concerns of every body or group who might be in need of securing, as their top-down notions of security fail to address the needs of particular communities. By better connecting community-specific security breakdowns with the resulting social practices of security enactment, we stand to discover how to build more community- and socially-situated security interventions. In addition, further work could also discuss the political charge of toolkit-making, through, for example, an ethnographic account of the development of a particular resource. This work could lead to deeper understanding of how threats are framed, and why particular adversaries are chosen to meet rhetorical goals around the work of security.

## 6 CONCLUSION

Cybersecurity toolkits are both technological solutions and reflections of diverse values with regard to (cyber)security and surveillance. They both recommend practices, and embody desires for security that dominant practices and default settings do not address. Through our analysis of a set of cybersecurity toolkits, we arrive at the notion of *differential vulnerabilities*, an understanding of security that recognizes safety as socially contingent, adversaries as unstable figures, and risk as differentially applied based on markers of relational position (e.g. class, race, religion, gender, geography, experience). Considering differential vulnerabilities offers both a pragmatic design concern for the development of future security resources, as well as a critical concept for security discourses.

## 7 ACKNOWLEDGMENTS

This work was supported by a grant from the UC Berkeley Center for Long-Term Cybersecurity and by NSF grants 1453329, 1423074, 1523579, DGE 1752814. We thank the reviewers for their helpful feedback.

## 8 REFERENCES

[1] Norah Abokhodair, Adam Hodges, and Sarah Vieweg. 2017. Photo Sharing in the Arab Gulf: Expressing the Collective and Autonomous Selves. In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW '17, 696–711. https://doi.org/10.1145/2998181.2998338

[2] Sara Ahmed. 2014. The Cultural Politics of Emotion. Edinburgh University Press, Edinburgh.

[3] Madeleine Akrich. 1992. The De-Scription of Technical Objects. In Shaping Technology Building Society: Studies in Sociotechnical Change, Wiebe Bijker and John Law (eds.). MIT Press, 205–224.

[4] Jeffrey Bardzell and Shaowen Bardzell. 2015. The user reconfigured: on subjectivities of information. In Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives (AA '15), 133-144. http://dx.doi.org/10.7146/aahcc.v1i1.2129

[5] Eric P S Baumer and Jed R Brubaker. 2017. Post-userism. In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems - CHI '17, 6291–6303. https://doi.org/10.1145/3025453.3025740

[6] Bennet Berger. The Survival of a Counterculture: Ideological Work and Everyday Life Among Rural Communards. University of California Press, 1981.

[7] Michel de Certeau. 1984. The practice of everyday life. Berkeley: University of California Press.

[8] Danielle Keats Citron. 2014. Hate Crimes in Cyberspace, Harvard University Press.

[9] Sauvik Das, Adam D.I. Kramer, Laura A. Dabbish, and Jason I. Hong. 2015. The Role of Social Influence in Security Feature Adoption. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '15), 1416-1426. https://doi.org/10.1145/2675133.2675225

[10] Christopher A. Le Dantec, Erika Shehan Poole, and Susan P. Wyche. 2009. Values as lived experience: Evolving value sensitive design in support of value discovery. In *Proceedings of the 27th international conference on Human factors in computing systems - CHI 09*, 1141. https://doi.org/10.1145/1518701.1518875

[11] Paul Dourish and Ken Anderson. 2006. Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction* 21, 3: 319–342. https://doi.org/10.1207/s15327051hci2103_2

[12] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08), 1065-1074.: https://doi.org/10.1145/1357054.1357219

[13] Serge Egelman, Serge, and Eyal Peer. 2015. The myth of the average user: Improving privacy and security systems through individualization. Proceedings of the 2015 New Security Paradigms Workshop. https://doi.org/10.1145/2841113.2841115

[14] Batya Friedman, Peter H. Kahn, and Alan Borning. 2008. Value Sensitive Design and Information Systems. In The Handbook of Information and Computer Ethics, Kenneth Einar Himma and Herman T. Tavani (eds.). John Wiley & Sons, Inc., 69–101.

[15] Jean Hardy and Silvia Lindtner. 2017. Constructing a Desiring User: Discourse, Rurality, and Design in Location-Based Social Networks. In Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing - CSCW '17, 13–25. https://doi.org/10.1145/2998181.2998347

[16] Lara Houston, Steven J Jackson, Daniela K Rosner, Syed Ishtiaque Ahmed, Meg Young, and Laewoo Kang. 2016. Values in Repair. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems - CHI '16*, 1403–1414. https://doi.org/10.1145/2858036.2858470

[17] Tung-Hui Hu. 2015. A Prehistory of the Cloud. MIT Press.

[18] Haiyan Jia, Pamela J. Wisniewski, Heng Xu, Mary Beth Rosson, and John M Carroll. 2015. Risk-taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing - CSCW '15, 583–599. https://doi.org/10.1145/2675133.2675287

[19] Cory Knobel and Geoffrey C. Bowker. 2011. Values in design. Communications of the ACM 54, 26. https://doi.org/10.1145/1965724.1965735

[20] Steven J. Jackson. 2014. Rethinking Repair. In *Media Technologies: Essays on Communication, Materiality, and Society*, Tarleton Gillespie, Pablo J. Boczkowski and Kirsten A. Foot (eds.). The MIT Press, 221–240. https://doi.org/10.7551/mitpress/9780262525374.003.0011

[21] Nassim JafariNaimi, Lisa Nathan, and Ian Hargraves. 2015. Values as Hypotheses: Design, Inquiry, and the Service of Values. *Design Issues* 31, 4: 91–104. https://doi.org/10.1162/DESI_a_00354

**[22]** Zeus Leonardo. 2004. The Color of Supremacy: Beyond the discourse of "white privilege." Educational Philosophy and Theory 36, 2: 137–152. https://doi.org/10.1111/j.1469-5812.2004.00057.x
**[23]** Helen Nissenbaum. 2001. How computer systems embody values. Computer 34, 3: 120–119. https://doi.org/10.1109/2.910905
**[24]** Helen Nissenbaum. 2005. Where Computer Security Meets National Security. *Ethics of Information Technology* 7, 2: 61–73.
**[25]** Bryan D. Payne and W. Keith Edwards. 2008. A Brief Introduction to Usable Security. IEEE Internet Computing 12, 3: 13–21. https://doi.org/10.1109/MIC.2008.50
**[26]** Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: user attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12), Article 3 , 14 pages. http://doi.acm.org/10.1145/2335356.2335360
**[27]** Jennifer A. Rode. 2010. The roles that make the domestic work. In Proceedings of the 2010 ACM conference on Computer supported cooperative work (CSCW '10). 381-390. https://doi.org/10.1145/1718918.1718984
**[28]** Daniela K. Rosner and Morgan Ames. 2014. Designing for repair?: infrastructures and materialities of breakdown. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing - CSCW '14*, 319–331. https://doi.org/10.1145/2531602.2531692
**[29]** Katie Shilton, Jes A. Koepfler, and Kenneth R. Fleischmann. 2014. How to see values in social computing: Methods for Studying Values Dimensions. In Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW '14), 426–435. https://doi.org/10.1145/2531602.2531625
**[30]** Yang Wang. 2017. The Third Wave? Inclusive Privacy and Security. In Proceedings of the 2017 New Security Paradigms Workshop - NSPW 2017, 122–130. https://doi.org/10.1145/3171533.3171538
**[31]** Alma Whitten and J.D. Tygar. 1999. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium, 169–184.
**[32]** Langdon Winner. 1980. Do Artifacts Have Politics? Daedalus 109, 1: 121–136.
**[33]** Steve Woolgar. 1990. Configuring the User: The Case of Usability Trials. The Sociological Review 38, 1_suppl: 58–99. https://doi.org/10.1111/j.1467-954X.1990.tb03349.x
**[34]** Shundan Xiao, Jim Witschey, and Emerson Murphy-Hill. 2014. Social influences on secure development tool adoption: why security tools spread. In Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing (CSCW '14). 1095-1106. https://doi.org/10.1145/2531602.2531722

## 8 APPENDIX: TOOLKIT REFERENCES

**[35]** Heartmob. https://iheartmob.org/
**[36]** Best Practices for Conducting Risky Research and Protecting Yourself from Online Harassment. https://datasociety.net/output/best-practices-for-conducting-risky-research/
**[37]** Facebook Security Basics / Take the Security Checkup. https://www.facebook.com/about/basics
**[38]** Integrated Security. http://www.integratedsecuritymanual.org/
**[39]** Stop.Think.Connect. https://www.stopthinkconnect.org/research-surveys
**[40]** DHS Stop.Think.Connect Toolkit. https://www.dhs.gov/stopthinkconnect
**[41]** Holistic Security. https://holistic-security.tacticaltech.org/
**[42]** Surveillance Self-Defense. https://ssd.eff.org/en
**[43]** Digital Security Helpline . https://www.accessnow.org/help/
**[44]** Low orbit ion cannon. https://en.wikipedia.org/wiki/Low_Orbit_Ion_Cannon
**[45]** Security In-A-Box. https://securityinabox.org/en/
**[46]** My and My Shadow. https://myshadow.org/resources
**[47]** Crash Override / Prevent Doxing guide. http://www.crashoverridenetwork.com/preventingdoxing.html
**[48]** Digital First Aid Kit. https://www.digitaldefenders.org/digitalfirstaid/
**[49]** Digital Security 101 Video Tutorials. https://www.equalitylabs.org/internet-freedom-and-digital-security/
**[50]** Center for Media Justice / Digital Security Workshops. http://centerformediajustice.org/grassroots-digital-security-training-series/
**[51]** SecureDrop. https://securedrop.org/
**[52]** Simply Secure. https://simplysecure.org/what-we-do/
**[53]** CryptoParty. https://www.cryptoparty.in
**[54]** Advocacy Assembly. https://advocacyassembly.org/en/partners/securityfirst/
**[55]** Speak Up & Stay Safe(r): A Guide to Protecting Yourself From Online Harassment. https://onlinesafety.feministfrequency.com/en/
**[56]** Resisting Doxing & Protecting Privacy: Resources For Vulnerable People. https://www.ohshitwhatnow.org/2017/06/26/resisting-doxing-protecting-privacy-resources-vulnerable/
**[57]** Sprout Distro Security Zines. https://www.sproutdistro.com/catalog/zines/security/

**[58]** DIY Guide to Feminist Cybersecurity & DIY Cybersecurity for Domestic Violence. https://hackblossom.org/cybersecurity/
**[59]** C.O.A.C.H, Automated Cybersecurity Helper. http://www.crashoverridenetwork.com/coach.html
**[60]** Tor. https://www.torproject.org/docs/documentation.html.en, https://trac.torproject.org/projects/tor/wiki/TorRelayGuide
**[61]** Mozilla's Privacy Not Included. https://advocacy.mozilla.org/en-US/privacynotincluded/
**[62]** CSO IoT security basics: Survival Guide. Organizer/producer: International Data Group CSO Magazine. http://images.techhive.com/assets/2017/05/16/cso_guide_iot_0516.pdf, https://www.csoonline.com/article/3196246/internet-of-things/the-cso-iot-security-basics-survival-guide.html?upd=1517892368323
**[63]** Google's Data Liberation/Data Liberation Front. https://sites.google.com/a/dataliberation.org/www/home , http://dataliberation.blogspot.com/
**[64]** Do it yourself Online Safety guide. https://chayn.co/safety/
**[65]** Journalist's Toolkbox. https://www.journaliststoolbox.org/2018/01/26/free_speechfirst_amendment_issues_1/
**[66]** Imminent Threat Solutions / Digital Security. https://www.itstactical.com/digicom/security/cyber-csi-digital-forensics-fingerprints-leave-behind/
**[67]** KiwiFarms guide for online self protection. https://kiwifarms.net/threads/cybersecurity-101.11731/
**[68]** A 70-Day Web Security Action Plan for Artists and Activists Under Siege. https://medium.com/@TeacherC/90dayactionplan-ff86b1de6acb
**[69]** Chicago Police Department coaches officers on how to avoid the same social media surveillance they themselves employ. https://www.muckrock.com/news/archives/2018/apr/11/cpd-social-media/
**[70]** That One Privacy Guy's - Guide to Choosing the Best VPN (for you). Organizer/producer: That One Privacy Site. https://www.reddit.com/r/VPN/comments/4iho8e/that_one_privacy_guys_guide_to_choosing_the_best/ , https://thatoneprivacysite.net/vpn-comparison-chart/
**[71]** Center for Development of Security Excellence toolkits and resources. https://www.cdse.edu/toolkits/cybersecurity/index.php
**[72]** Center for Internet Security toolkit. https://www.cisecurity.org/ms-isac/ms-isac-toolkit/
**[73]** AICPA "Top 20 Cybersecurity Tips". https://www.aicpa.org/interestareas/privatecompaniespracticesection/qualityservicesdelivery/informationtechnology/cybersecurity-checklist.html
**[74]** NSA's Media Destruction Guidance. https://www.nsa.gov/resources/everyone/media-destruction/
**[75]** "An In-Depth Guide to Personal Cybersecurity". https://medium.com/@nickrosener/an-in-depth-guide-to-personal-cybersecurity-be98ba47c968

Received April 2018; revised July 2018; accepted September 2018.