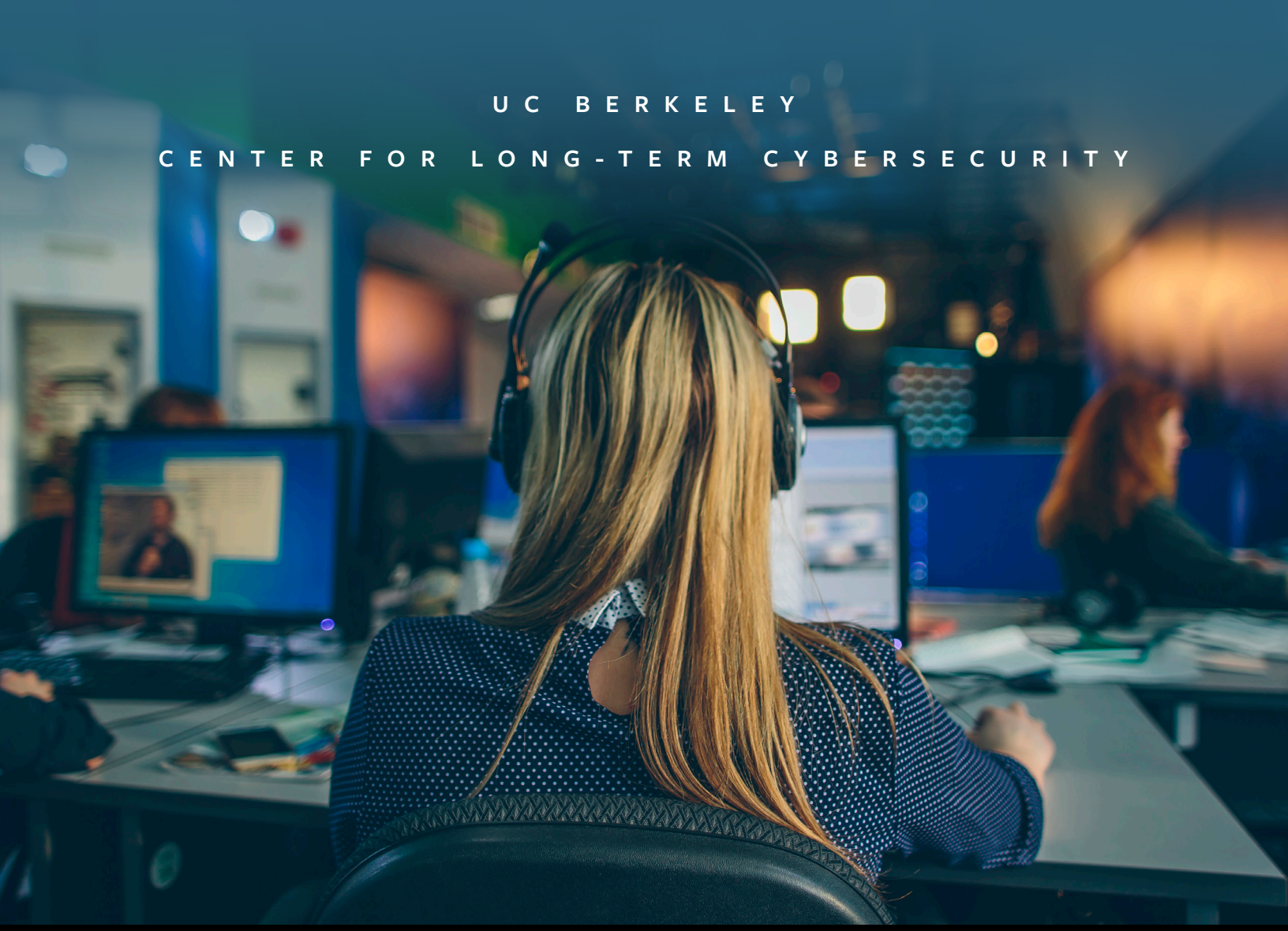
UC BERKELEY
CENTER FOR LONG-TERM CYBERSECURITY



CLTC WHITE PAPER SERIES

An Evaluation of Online Security Guides for Journalists

KRISTIN BERDAN

CLTC WHITE PAPER SERIES

An Evaluation of Online Security Guides for Journalists

KRISTIN BERDAN
Research Fellow, Center for Long-Term Cybersecurity,
University of California, Berkeley

JANUARY 2021

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

CENTER FOR LONG-TERM CYBERSECURITY

University of California, Berkeley

Contents

Executive Summary

Attacks on journalists and freedom of the press have increased markedly over the past several years around the globe. Covering protests in the aftermath of the murder of George Floyd by police officers in Minneapolis in 2020, journalists experienced a significant increase in attacks from an already high number of incidents. The attacks run the gamut from personal online attacks on and harassment of journalists, to damage and confiscation of journalists' equipment by law enforcement, to arrest and detention of reporters covering protests and other events. Yet most journalists are not adopting online security practices that could help defend against such attacks.

This paper posits that a key reason why journalists do not take sufficient action to protect themselves online is that there is an overwhelming amount of security advice on the internet, most of which is difficult for journalist-readers to understand or translate into practice, and difficult for the authors of the advice to keep up to date. Most guides do not account for journalists' busy schedules and time-pressured work cycles. Journalists also operate in an increasingly hostile environment, even in countries with democratic governments and some historical guarantees of freedom of the press and rule of law.

The analysis in this paper seeks to answer three questions: (1) what security advice exists for journalists specifically? (2) is the existing advice effective? and (3) what is the best way to measure that? We report findings from an analysis of 33 online security guides available on the public internet that are geared toward journalists. We documented nearly 300 separate pieces of advice provided in these guides, including recommendations for roughly 200 different tools. We catalogued each separate piece of security advice, recorded how often a piece of advice appeared across all the guides, and organized the advice into categories. We also evaluated each guide according to a set of quantitative and qualitative criteria to gauge each guide's efficacy in improving journalistic security.

As detailed in this paper, the analysis revealed that most online security guides for journalists do not prioritize their content effectively, and provide no clear path for users to improve their security in a time-efficient way. The advice provided was also inconsistent across the guides. This paper concludes with recommendations to make guides and security education of journalists overall more effective:

1. *Always start with risk.* Help the journalist understand and assess the risk of their story or beat. Only then will the reader-journalist be receptive and curious about the tool or practice that is appropriate given their risk assessment.

2. *Integrate security practice with the journalist's workflow.* Journalists will allow only so much friction in their workflow, given the unceasing time pressure of publication. If they first recognize the threat, appropriately measure the risk, and then choose a tool or practice that they can work with on a daily basis, the chances of long-term success as a journalist who keeps themselves, their story, and their sources secure will rise significantly.

3. *Security as a competitive advantage.* The journalist who has secured their accounts and devices will be empowered to safely explore the darker corners of the internet to extract the information needed to tell the stories that help maintain democracy and freedom in society.

4. *Newsrooms and journalism schools should integrate security education into their programs.* Journalists could be more effective and their work would have more impact if they had institutional support for their online security, and if journalism schools graduated students with the skills to protect themselves and their stories, in addition to the investigative techniques to get the stories.

The digital age provides immense opportunities for investigative journalism, but it also offers thousands of ways in which journalists can get trolled or threatened. Security education for journalists must be contextually informed, prioritized, and actionable to be effective in facilitating journalists' critical role in democratic society.

"It used to be the news organizations that were attacked but now it is the journalists themselves as individuals."[1]

"The true quality of a nation's democracy can be measured by the security and safety of its journalists. When journalists can act without fear, secure in their person and in their profession, they are empowered to bring vital information to the people. They become agents of democracy and freedom. They serve as a watchdog over the institutions of society. They can convey accurately and objectively the actions and attitudes of the power brokers of society. In this way they are as vital as any other actor or institution in the democratic form of governance."[2]

1 Reporters Without Borders, "Online Harassment" 7.

2 Audronius Ažubalis, Lithuania's Minister for Foreign Affairs and a former journalist. Horsley 3.

Introduction

In February 2019, *Slate* published a story by investigative reporter April Glaser about an e-commerce site operated to raise revenue for the Proud Boys,[3] a U.S.-based far-right group that engages in violent actions to promote misogynistic, anti-Muslim, white supremacist ideology.[4] Glaser's article exposed the challenges that the Proud Boys faced in using commercial payment processing services to fund their activities. As a result, Glaser later recounted, she faced an onslaught of harassing emails and direct messages from Proud Boys supporters on social media, and she was doxxed.[5] Glaser's admirable reaction to this treatment included publishing an article advising journalists on how to protect themselves from online harassment. Her guidance in that article, while effective and extremely practical, joined an abundance of security advice already available to journalists on the public internet.

Global surveys indicate that journalists do have some awareness of online threats.[6] Given the large number of online security guides available to help them protect themselves, why do they not do more to secure themselves and their work online, given they believe (and ample evidence supports this belief) that they are under attack? And why should we, as citizens, care?

Journalists learn about security practices through:

- informal interactions with colleagues,[7]
- workshops, typically of short duration,[8] and
- independent research, including through searches of the public internet using search engines.

This paper focuses on the results that a journalist might find using an internet search. We reviewed nearly three dozen online security guides for journalists and measured how much

3 Glaser, "It Just Got."
4 Southern Poverty Law Center.
5 Glaser, "13 Security Tips." "Doxxing" occurs when someone, with malicious intent, publicly posts online personally identifying information (such as a residential address) about an individual.
6 Westcott, "Journalist Safety."
7 Henrichsen, "Breaking Through" 332. See also LaForme ("Newsrooms by and large, especially small and regional papers, don't have the resources to invest in formalized training on this," Pitts said. "And so it falls to a more peer training model," where the "nerdiest person on the reporting team" or someone who shared a tool once and became known as an "expert" provides most of the training.")
8 Henrichsen, "Breaking Through" 335.

advice is given, to what extent that advice varies within and between guides, and whether the advice is presented in a prioritized and context-appropriate manner. As security education for journalists (both academic and professional) is rare, it is crucial that accurate and effective online advice is easily accessible to journalists who seek to protect themselves and their work online. This paper concludes that there is a high probability that journalists who access security guides via a simple internet search will find it challenging to effectively implement security advice for their particular professional context.

One factor that makes security education challenging for journalists is the significant time pressure under which journalists do their work: reporting today requires working within a deadline-driven, 24/7 news culture. Moreover, according to a recent survey, journalists operating in "technologically advanced market-oriented democracies" perceive greater time pressure compared to their colleagues in centralized economies, where the government is the primary source of information:

> [J]ournalists in those countries, which are technologically advanced, are most affected in that the working hours have increased substantially while the time to prepare stories has decreased. . . . These countries, moreover, are democracies where deliberation and exchange of opinions are seen as an asset, and as part of the social and political environment. It is in these countries that the engagement with the civic world is viewed as part of media's public service, and where participation in social and political matters is encouraged (Haas 2007; Carpentier 2011). The increased interaction with the audience, be it directly with readers or by gauging their interests and following their posts on social media, or posting on social media themselves, has substantially altered journalists' work pattern and working hours.[9]

Journalists are working longer hours in those democracies where they play a vital role as watchdog, protector, and skeptic.[10] That vital role is jeopardized by the dangerous confluence of increased threats and a lack of security. However, most journalists make the calculation that the perceived level of effort and time required to improve their security is not worthwhile. As one researcher wrote in 2009,

> Users perform an implicit cost/benefit calculation when deciding whether to follow security advice or not. The cost is the effort to follow the advice, while the benefit is avoidance of the harm that the attack might bring. The harm includes the monetary loss (if any) that victims endure, but also the time and effort they must spend resolving

9 Halliki and Josephi 404.

10 Henrichsen, "Breaking Through" 342.

> the situation with the [platform or organization where the user's account was compromised].[11]

Every moment a journalist spends on improving their security is potentially a moment lost to chasing a story, which may result in losing a scoop and/or income. A 2015 Pew Research survey bears this out, as 97% of journalists surveyed said that "the benefits of digital communication like email and cellphones outweigh the risks. Just 3% say the risks outweigh the benefits."[12]

And yet attacks on journalists are increasing. Margaret Sullivan, former *New York Times* public editor, wrote "it's turning out to be the administration of . . . unprecedented attacks on a free press."[13] Readers of this white paper after the year 2020 may be surprised to learn that Sullivan wrote this in 2013 about the Obama administration's actions to clamp down on investigative journalism practices in the United States.[14] During the Trump Administration, attacks on journalists and freedom of the press increased markedly.[15] Covering protests in the aftermath of the murder of George Floyd by police officers in Minneapolis in 2020, journalists experienced a significant increase in attacks from an already high number of incidents.[16] The attacks run the gamut from personal online attacks on and harassment of journalists, to reporting equipment damaged or confiscated, to journalists being detained and arrested.[17]

Surveillance of journalists' activities is pervasive. Since 9/11, the U.S. government, from the federal to state and local levels, has engaged in broad surveillance of communications traffic, and the Obama Administration combined surveillance with an unprecedented practice of prosecution of sources who disclosed information to investigative reporters.[18] Under the Trump Administration, hostility toward the free press grew significantly.[19] In addition to continued prosecution of government sources, the Administration has attacked the credibility of journalists, "interfered in the business of media owners, harassed journalists crossing U.S.

11 Herley 2.
12 Holcomb and Mitchell.
13 Sullivan.
14 For more on the Obama administration's hostility toward the press, see Henrichsen, "The Rise" 21.
15 Committee to Protect Journalists.
16 McCudden.
17 McCudden.
18 Downie and Rafsky.
19 See, e.g., Committee to Protect Journalists, citing "Trump's steady stream of verbal attacks, members of the press . . . regularly booed at Trump rallies, and reporters named in his tweets . . . repeatedly harassed online. There also have been credible threats to news organizations."

borders, and empowered foreign leaders to restrict their own media."[20] Scholar Jennifer Henrichsen at the University of Pennsylvania noted in 2020,

> Over the last several years, numerous journalists and news organizations have reported incidents in which their communications have been hacked, intercepted, or retrieved. In 2014, Google security experts found that 21 of the world's 25 most popular media outlets were targets of state-sponsored hacking attempts, and many journalists have watched helplessly as hackers took control of their social media accounts, targeting confidential information in their internal servers. When journalists' digital accounts are vulnerable to hacks or surveillance, news organizations, journalists, and their sources are at risk, and journalists' ability to carry out their newsmaking function is reduced.[21]

Journalists are cognizant of the threat. Even before the commencement of the Trump Administration, many journalists were aware of at least some of the online threats they face. In 2015, a survey found that "[a]bout two-thirds of investigative journalists surveyed (64%) believe that the U.S. government has probably collected data about their phone calls, emails or online communications, and eight-in-ten believe that being a journalist increases the likelihood that their data will be collected."[22] Henrichsen noted that the journalists' held a variety of beliefs, ranging from technological ignorance to a mix of "fatalism and paranoia" to paralyzing "unreasonable paranoia."[23] The end result is that journalists are failing to secure themselves and their stories from online threats.[24] Researchers interviewing journalists in 2015 described the "mental model" of journalists when it comes to security as "a type of 'security by obscurity': the belief one need not take particular security precautions unless one is involved in work that is sensitive enough to attract the attention of government actors."[25] In the year of this writing (2020), there is ample evidence that one's security risk is determined by who you are as well as what you do: journalists who are women and people of color are disproportionately targeted for online harassment.[26]

20 Committee to Protect Journalists. Journalists in countries other than the United States also face increased dangers. For example, a 2017 report identified journalists as the no. 3 target of Russian government surveillance, behind diplomats and U.S. Democrats. See Satter.

21 Henrichsen, "Breaking Through" abstract.

22 Holcomb and Mitchell.

23 Henrichsen, "Breaking Through" 332.

24 From a survey of journalists conducted in 2018: "More than half of journalists (54%) and newsrooms (52%) fail to secure their communications." Owen 4.

25 McGregor and Watkins 39.

26 From 2018, see UNESCO. From 2020, see Duncan, quoting an Al Jazeera+ senior producer and presenter: "I don't think you can be a woman or person of color in the 21st century and not be thinking about harassment and online abuse. It doesn't matter what you cover. I've seen it in all spaces."

From conducting internet searches, we know that security guides for journalists are in large supply. In the general population, in spite of a multitude of sources providing security advice, "user adoption of protective behaviors remains inconsistent at best."[27] This pattern is observed in the journalist population as well.[28]

We gathered 33 publicly available online guides aimed at improving journalists' security. We documented nearly 300 separate pieces of advice, including recommendations for about 200 different apps or web-based services ("tools"). We catalogued each separate piece of security advice, and tallied how often a piece of advice appeared across all of the guides. We organized the advice into categories. We evaluated each guide according to a set of criteria (described below) to gauge each guide's efficacy in improving journalistic security.[29]

We observe that most guides do not prioritize their content in any way, and provide no path for a time-pressured journalist to follow to improve their security in an efficient way. We also conclude that the best guides have certain characteristics, which help to make the guide more effective, and we share those in this paper.

This analysis sought to answer three questions: (1) what security advice exists for journalists specifically? (2) is the existing advice effective? and (3) what is the best way to measure that? We use three methods:

1. Advice census: During the period from June–July 2020, I used Google to search for security guides aimed at journalists, selected by their search rankings and English-language format, and capped the list at 33. We (two researchers) then coded and catalogued each piece of advice from the guides.
2. Guide evaluation: I evaluated the guides using qualitative criteria adapted from several wide-ranging sources.
3. Node maps: We developed two node maps: one showing all external links from each guide, and one showing referrals between guides so we can see which guides are perceived as authoritative among the publishers of security guides for journalists.

27 Redmiles et al. 89.

28 Holcomb and Mitchell.

29 All of our research data is publicly available at this site: https://sites.google.com/view/journosec-guides/home.

Methodology

BACKGROUND AND RELATED RESEARCH

In 2017, Google researchers published a paper that analyzed general digital security advice from security experts for the non-technical user.[30] It found a lack of consensus and agreement on priorities, and even confusion among the expert group on what users should do to stay safe online. The researchers gathered the advice and then coded it, parsing each separate piece of advice. They grouped the advice by category and determined the ten most popular pieces of advice. The researchers then developed a set of criteria to define good general security advice:

1. **Effective.** Good advice, if followed by a user, should actually improve the user's security situation and lead to better security outcomes.
2. **Actionable.** Good advice should be easy for a user to remember and apply when needed, and it should not overly interfere with a user's primary goals.
3. **Consistent.** Good advice should be both internally consistent—in that it should not cause confusion with or subsume other advice in the whole set of advice—and presented consistently—in that it should be phrased similarly each time a user hears it and should change as little as possible over time (as long as it remains effective).
4. **Concise.** The set of advice as a whole should be as small as possible. Less advice is easier for users to remember than more advice, and less advice to follow means it is easier to follow all of it.[31]

Although the focus of Reeder et al.'s paper is general security advice and not advice that is contextualized for any particular audience, it includes this relevant observation:

> A great deal of security advice is available to those looking for it. Many service providers, enterprises, universities, and other organizations offer advice in the form of tips and training on how to stay safe online. One of the most comprehensive and authoritative sources of advice intended for nontechnical users is provided by US-CERT (www.us-cert.gov/ncas/tips), which by our count spans 57 pages and offers 534 individual pieces of advice. Recommendations range from common advice like "keep

30 Reeder et al.
31 Reeder et al. 61.

> your antivirus software current" to less common advice like "consider challenging service providers that only use passwords to adopt more secure methods." With such a large set of advice, it might be unclear to many users where to get started, to whom the advice applies, and why following the advice will help.[32]

Complementary findings have been produced in research focused on online advice on the topic of security and privacy for general audiences. In 2020, Redmiles et al. looked at 1,264 documents of online security and privacy advice and evaluated the lot according to a set of qualitative criteria focused on the "comprehensibility, perceived actionability, and perceived efficacy" of that advice.[33] This research, too, coded each separate piece of security advice and categorized it. They concluded that while most advice was "somewhat actionable, and somewhat comprehensible," the lack of prioritization of such a large amount of advice made it less effective than it otherwise could have been because most users would struggle to know where to start, "left to fend for themselves, navigating through a sea of reasonably well-crafted but poorly organized advice."[34]

SCOPE OF THIS PAPER

Guides aimed at improving journalists' online security represent a specific subset of online security guides aimed at the general population. I identified this advice by doing what a journalist might do: conducting internet searches.[35] I purposefully did not ask security experts for their recommendations for the best guides or advice because most journalists do not have access to security experts. I also discovered some security guides because they were cross-referenced in others (see node map section below). Most of the guides are written for journalists, but I did include three guides written for general audiences because of their popularity.[36] We settled on a total list of 33 online security guides, from sources such as journalist advocacy organizations (e.g., the Committee to Protect Journalists), corporations (e.g., Facebook), news organizations (e.g., *New York Times*), and civil liberties organizations (e.g., Electronic Frontier Foundation). This paper makes no claim to this being a complete or comprehensive list because, in addition to the large number of guides that are publicly available:

32 Reeder et al. 56.

33 Redmiles et al. 89.

34 Redmiles et al. 90.

35 See Machill and Beiler for the general proposition that search engines are an important tool in journalistic research, and Google's search engine is the most popular among journalists.

36 (1) Security in a Box's "Digital Security Tools and Tactics," (2) Consumer Reports' (formerly Citizen Lab's) "Security Planner," and (3) Rapid Response Network and CiviCERT's "Digital First Aid."

- We examined guides only written in English.
- I sought only guides that are available on the public internet. This means I did not include proprietary training materials offered by organizations for a fee.
- I limited our review to written materials and did not consider other formats, such as video.

QUANTITATIVE EVALUATION

Advice Census

We evaluated the guides using both qualitative and quantitative criteria. The first step of the quantitative evaluation entailed parsing each individual piece of advice in every guide (the "advice census"). Two members of the research team reviewed the guides and annotated them, extracting each piece of advice. One member of the research team also spot-checked the work of the other team member. Ultimately, we identified 297 pieces of advice, described by Redmiles et al. as "unique advice imperatives targeting end users."[37] (The complete list of guides and the set of advice imperatives can be found at https://sites.google.com/view/journosec-guides/home). Some guides found through our internet searches were not fully analyzed because, upon further examination, they were "disqualified" in some way. For example, one website turned out to be marketing collateral for an app, and another contained only recommendations for policymakers, rather than advice for journalists themselves. We retain them in the list because nonresponsive search results like these often make up part of the results for the quotidian online searches that people do, and they take valuable time on the part of the searcher to sift through to find the relevant resources.

As the next step, we grouped the 297 pieces of advice into categories. These were derived by placing together advice imperatives that covered the same subject matter. Categories and examples are found in Table 1.[38]

37 Redmiles et al. 92.

38 We developed these categories by reviewing the types of advice and grouping them according to common subject-matter. They are similar but not identical to the categories that emerged from Redmiles et al.'s review of security advice. See Redmiles et al. 93.

TABLE 1. CATEGORIES AND EXAMPLES

CATEGORY	EXAMPLES
Access	Set up a lockscreen on your phone
Account activity	Disable inactive accounts
Account settings	Disable location tracking by social media apps
Authentication	Create strong passwords
Border crossing	Log out of all accounts before approaching any border control area
Communications	Use a secure platform to communicate with sources
Data back-up	Back-up data regularly from your devices to the cloud
Data management	Separate work and personal accounts
Encryption	Encrypt your data storage
Equipment care	Enable power and back-up power appropriately
General	Minimize data gathered about you by turning off wifi
Malware	Do not download suspicious documents onto your devices
Meta	Check the "last updated" date on guides to see that the advice is current. Things change fast
Metadata	Remove metadata from files provided by sources and images you take with your phone before sharing or publishing them
Operational security	Avoid lending your phone to others
Phishing	Be wary of messages that urge you to do something quickly or appear to be offering you something that seems too good to be true
Legal	Always research the law to ensure encryption is legal in the country you are living in or travelling to
Protect sources	No journalist should offer a promise of confidentiality until weighing the possible consequences; if a journalist or media organization does promise confidentiality, the commitment carries an important ethical obligation
Psycho-social support	Create a network of supportive colleagues, family, and friends
Risk assessment	Do a risk assessment before you start your assignment
Social media	On your profiles (e.g., Facebook), consider replacing your real ID with a nickname or pseudonym
Software updates	Apply system and software updates
Tools	Use Signal for encrypted messaging
VPNs	Use a virtual private network (VPN) to access blocked services

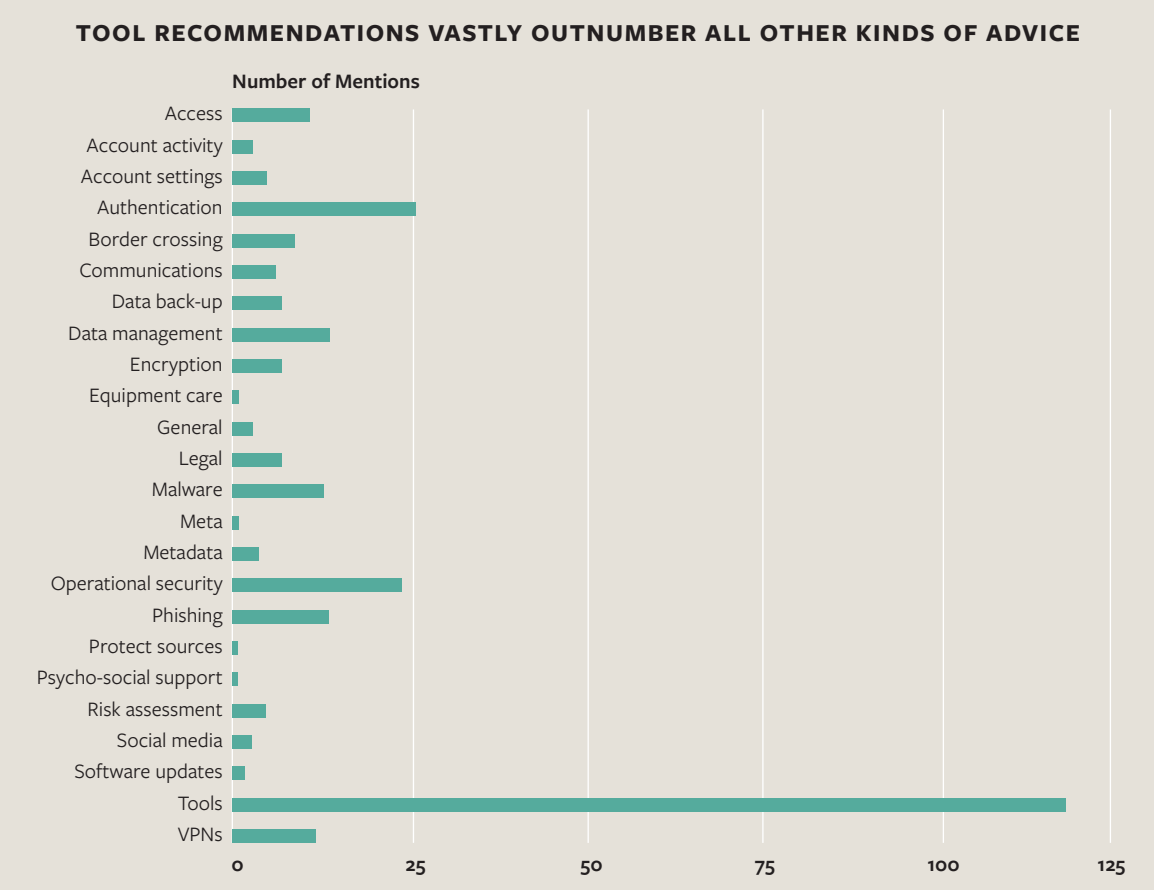


Fig. 1. Number of mentions of each category of advice across all guides.

I also tallied how often each piece of advice was mentioned across the entire set of guides. For example, the advice imperative to "use a VPN to access the web when using a public network" appears in 12 of the 33 guides.

Guide Referral Map

Initially in this research, we wanted to determine usage as a measure of each guide's "popularity." In considering how to measure usage or popularity, we considered and then discarded several ideas.[39] Instead, we noticed in our review that many of these sites link to

39 Rejected methods for measuring guide usage or popularity include: (1) Google Analytics data: most sites that advise journalists on security intentionally do not enable analytics to measure usage, so that was not an option; (2) Alexa, a widely used site-ranking service, ranks only TLDs and not subpages of a domain, so this was not going to work for guides that are located as a section of a larger organization's site or a news site; and (3) Google's "LINK" search operator: this was deprecated in 2017 and, while still usable, is no longer accurate or reliable.

each other, as a sort of friendly referral from one guide to another. I viewed this as a type of unofficial recommendation or endorsement by the community for that particular guide, and we show the links as an interactive node map of interguide referral at https://sites.google.com/view/journosec-guides/home/guide-to-guide-referrals-map.[40]

TABLE 2. GUIDE-TO-GUIDE REFERRALS

GUIDE	REFERRALS
Electronic Frontier Foundation, Surveillance Self-Defense for Journalists	10
Security in a Box, Digital Security Tools & Tactics	7
Freedom of the Press Foundation, Guides & Training	6
Access Now, Guide to Safer Travel	4
PEN, Harassment Field Manual, Consumer Reports' Security Planner (tied)	3
NICAR, Introduction to Digital Security for Journalists Handout (NICAR 2018)	2
Committee to Protect Journalists, Journalist Security Guide	2
Rapid Response Network and CiviCERT, Digital First Aid	2
OpenNews and contributors, The Field Guide to Security Training in the Newsroom	1
InterNews, Safer Journo: Digital Security Resources for Media Trainers	1
Rory Peck Trust, Digital Security Guide for Journalists	1

Twitter Mentions

Using Twitter's Tweetdeck,[41] I tallied the number of tweets and retweets for each guide for the period from January 2015 (which is the earliest date possible to search through Tweetdeck) through October 2020. I did not review the content of any mentions. I included English and non-English language mentions. I also did not exclude tweets by the authoring organization. This is an extremely rough snapshot of the uptake of such guides in the Twitterverse, a place where journalists increasingly turn (just like the rest of us) for both personal and professional communications and information-sharing.

40 We extracted all referral links from each guide, and then sorted them according to whether they were referrals to another guide or not. The entire dataset is available here: https://sites.google.com/view/journosec-guides/home.

41 https://tweetdeck.twitter.com.

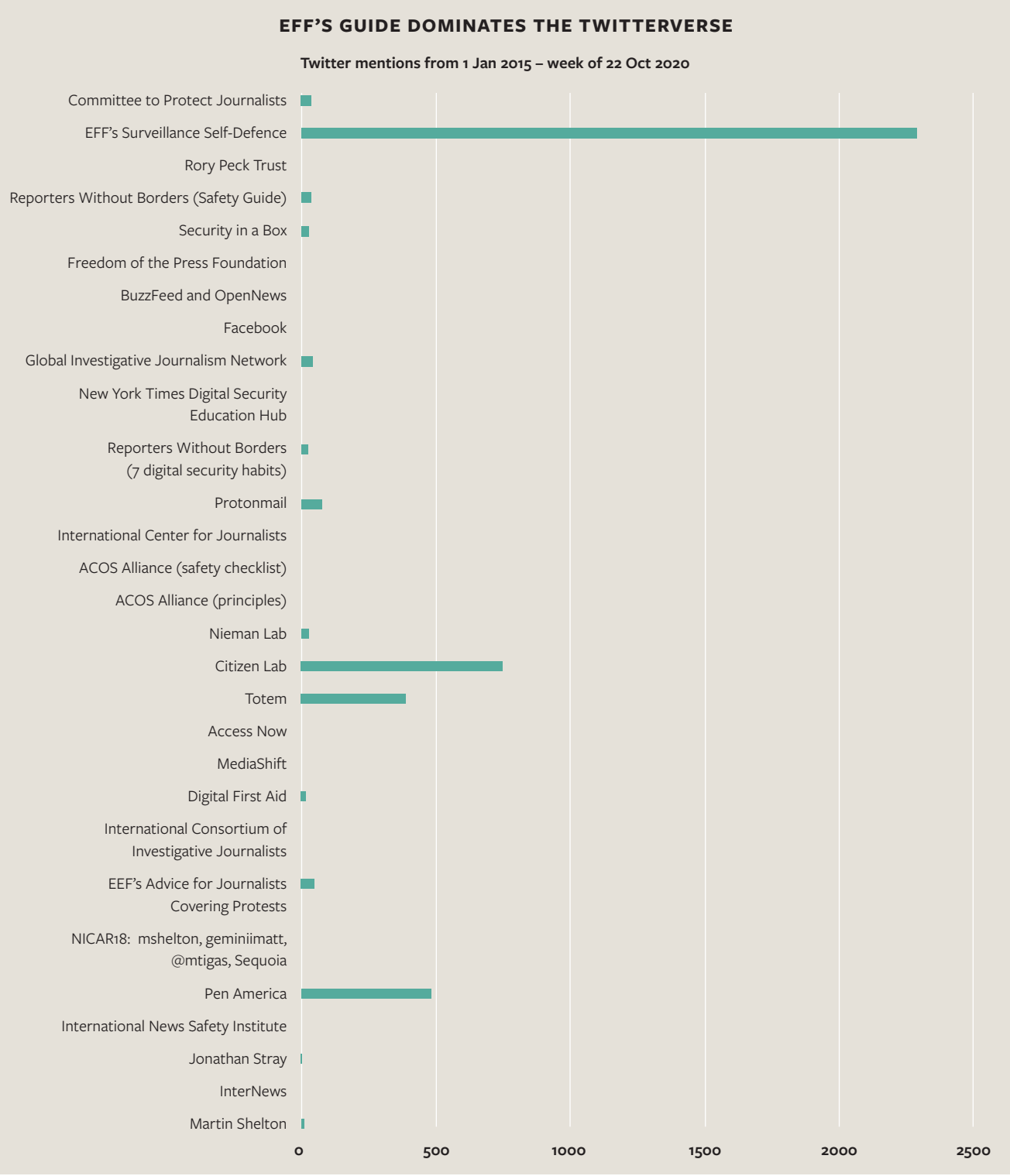


Fig 2. Number of Twitter mentions of each guide between 1 January 2015 and 22 October 2020.

QUALITATIVE EVALUATION

I next evaluated each guide based on the quality of security advice offered to journalists. This was a different challenge than carrying out a quantitative census of advice imperatives. Building on prior research, I established the following criteria for effective security advice for a journalistic audience:

CATEGORY	METRIC
1. Effective[42]	If the journalist takes the steps recommended, will it actually improve their security? This is important because if it does not make a difference in improving journalists' security, then it is not worth doing.
2. Actionable[43]	To what extent is the advice easy for a user to remember and apply when needed? To what extent does it not overly interfere with a journalist's primary goals? This is important because a journalist is more likely to adopt advice that is easy to carry out and does not interfere with their workflow.
3. Consistent[44]	To what extent is the advice both internally consistent—in that it does not cause confusion with or subsume other advice in the whole set of advice—and presented consistently—in that it is phrased similarly each time a user hears it and changes as little as possible over time (as long as it remains effective)? This is important because consistency helps make advice easier for users to understand, remember, and follow.
4. Concise[45]	To what extent is the advice communicated clearly and as briefly as possible without eliminating any essential elements?

In addition to the foundational qualitative characteristics above, I created several new criteria. These criteria are derived from a broad range of sources, as explained below:

42 "Good advice, if followed by a user, should actually improve the user's security situation and lead to better security outcomes." Reeder et al. 61. See also Redmiles et al. 92: "The efficacy questionnaire evaluated, for each advice imperative, Perceived efficacy: whether the expert believed that a typical end user following this advice would experience an improvement in, no effect on, or harm to their security."

43 "Good advice should be easy for a user to remember and apply when needed, and it shouldn't overly interfere with a user's primary goals." Reeder et al. 61. Redmiles et al. asked guide readers to determine "perceived actionability" by looking at four "sub-metrics": confidence, time-consumption, disruption, and difficulty. (92)

44 "Good advice should be both internally consistent—in that it should not cause confusion with or subsume other advice in the whole set of advice—and presented consistently—in that it should be phrased similarly each time a user hears it and should change as little as possible over time (as long as it remains effective)." Reeder et al. 61. To the extent that consistent advice minimizes confusion, it could be considered an element of the "comprehensibility" criteria in Redmiles et al. (93).

45 "The set of advice as a whole should be as small as possible." Reeder et al. 61. Redmiles et al. plead for "a strong commitment among security advice givers to minimality and practicality." (101)

CATEGORY	METRIC
Free and open source software (FOSS) advocacy	Does the site promote the use of FOSS tools over proprietary tools as a way to stay safer online? (Y/N)

Free and open source software ("FOSS") refers to software that is available for free, and is licensed to users on expansive terms permitting users to use, copy, and modify the software via its source code, which is publicly shared.[46] Examples of FOSS that are often recommended to journalists in online guides are applications like Signal[47] (for secure messaging) and Tor[48] (for anonymous browsing). FOSS is recommended over proprietary software because publicly available source code is reviewable and auditable, so vulnerabilities or malware can be discerned by a broad community of security researchers.[49] In proprietary software (such as the Microsoft Windows operating system), source code is not made publicly available, so users must trust that vulnerabilities are getting fixed and malware is not embedded. However, there is a danger in relying on FOSS as inherently secure only because its source code is publicly available: there is no guarantee that anyone will in fact review it. One must examine whether researchers are focused on examining the source code for the particular FOSS and also whether vulnerabilities are reported and corrective actions taken to fix those vulnerabilities in a timely manner. This is beyond the ken of most journalists to determine, and certainly takes up valuable time. I added the FOSS category to evaluate whether the security guides explain this technical topic or not.

CATEGORY	METRIC
Cultural relevance	To what extent does the material explicitly allow for cultural differences and how they might impact one's digital security? (scale of 1-5, 1 being "not at all," and 5 being "extremely helpful")

This category is strongly influenced by the experience of staff at UC Berkeley's Citizen Clinic, a public-interest technology clinic where interdisciplinary student teams work with politically targeted client organizations in order to provide contextually informed, risk-appropriate security guidance. At the Clinic, every client engagement involves a comprehensive examination by the Clinic team of the environment in which the client operates. Specifically, the team examines the factors that the client can and cannot control or influence across seven areas:

46 Free and open source.
47 Signal Technology Foundation.
48 The Tor Project, Inc.
49 "To increase confidence that your operating system does not have potential surveillance 'backdoors', it should be 'open source'," advises the International News Safety Institute.

(1) political, (2) economic, (3) social, (4) technological, (5) legal, (6) environmental, and (7) military.[50] The Clinic team, informed by this assessment, can then assess the client's operations, identify security risks, and help the client implement effective and sustainable mitigation strategies. The Clinic has found that contextually informed security guidance is more likely to be adopted by clients when those providing the advice have a full understanding of the culture both of the organization itself and of the environment in which the organization operates. When such understanding is present, effective risk assessment and the provision of appropriate security advice is possible.

The category is also inspired by the Critical Lens Protocol for design prototyping developed by Stanford's d.school, which illuminates how conscious and unconscious bias influences a designer's perception.[51] Such biases can influence the drafting of security guides as well.

Henrichsen has pointed out that training journalists in security and technology is less effective when the trainer has limited understanding of local context.[52] Henrichsen also observed that "the focus on short-term workshops involving skill building and threat modeling with individual journalists has been less effective than building digital literacy, creating capacity, and facilitating agency among journalists."[53] If this is the case in an in-person training session, however short in duration, it is even more likely when the training is provided as a static webpage or PDF document. Henrichsen specifically recommends that:

> Information security trainers who design training sessions should contextualize and personalize the workshops and seminars to the risks, threats, and situations journalists face to ensure that the tactics and tools they learn are applicable to their situation and effective for their needs. Whenever possible, local information security trainers who understand the unique contexts, social norms, and regional languages should be utilized.[54]

CATEGORY	METRIC
Racial equity	To what extent does the material recognize and address the impact of race on the digital security of all participants in the investigative process, including journalists and sources? (Scale from 1–5)

50 Citizen Clinic.
51 Hasso Plattner.
52 Henrichsen, "Breaking Through" 334–335.
53 Henrichsen, "Breaking Through" 335.
54 Henrichsen, "Breaking Through" 343.

This category could be considered a subcategory of "context," above, but its importance merits a separate mention. An assessment of risk informs recommendations to improve security, but "[t]echnical and policy mitigations to cybersecurity challenges will never reach their full potential until systemic racism is addressed and diverse voices are reflected among our ranks at all levels."[55] A journalist's online security risk may be increased simply because of their skin color, even before accounting for a particular story or beat. To be truly comprehensive and maximally effective, security guides for journalists should take racial equity issues into account for every participant in the investigative process, including journalists and their sources.

CATEGORY	METRIC
Role of sources	To what extent does the material recognize and address the dependency of journalists on sources and how that impacts digital security? (scale of 1–5)

Henrichsen noted that previous research shows that "journalists choose their communication methods based on their source's comfort level and access to technology rather than the most technically sophisticated tool," meaning that "sources ultimately have the upper hand in the journalist–source relationship."[56] Combine that reliance with the near-constant time pressures under which journalists operate, and the most secure communications app in the world is likely to be unused in the face of a competitive deadline to "get the story." Therefore a security guide designed for journalists must recognize the important role of sources.

CATEGORY	METRIC
Risk assessment	To what extent does the material help journalists understand their risks and help them connect practices with their working needs? (scale of 1-5)

A central tenet of Citizen Clinic's approach to client engagement is to begin with a risk assessment.[57] Through an upfront evaluation, security gaps become visible, and contextually appropriate mitigations can be recommended that will be effective in reducing or eliminating those gaps. Suggesting irrelevant, unnecessary, or ineffective tools or practices will not improve the security of journalists. As Henrichsen noted:

> Failing to understand risks and tie practices to actual needs for carrying out one's work contribute to the inability to successfully adopt information security practices. As a

55 Stewart.
56 Henrichsen, "Breaking Through" 331.
57 Citizen Clinic.

> result, more digital security trainers are using exercises involving information mapping in their workshops and seminars. Not only have these exercises led to greater clarity among participants, but they have facilitated feelings of control among journalists, which in turn improves their psychological state and reinforces a desire to continue protective security behaviors.[58]

Therefore, I evaluated whether the security guides included instruction on conducting risk assessments, as well as whether this practice was given appropriate prominence and priority.

CATEGORY	METRIC
Personal protection	To what extent does the material improve the journalist's personal safety? (scale of 1–5)

A journalist's personal safety is the foundation upon which all other elements of "security" are built. To be truly effective, security guides must recognize the impact that online security practices can have in the "offline" world. There is a documented connection between online attacks and real-world violence perpetrated against journalists.[59] Henrichsen suggests that journalists place a priority on their own personal safety, and this can be a persuasive "point of entry" in getting journalists to adopt effective security measures.[60]

CATEGORY	METRIC
Story investigation	To what extent does the material improve the journalist's investigatory skills (providing a competitive advantage)? (scale of 1–5)

Another way to persuade journalists to adopt security practices is to show them that by doing so, they gain a competitive advantage: many defensive digital security practices (such as keeping personal information private) can be turned and used as highly effective investigatory techniques (such as searching the public internet for personal information on targets or sources in order to pitch or build a story).[61] This combination of benefits played out in a course taught to first-year journalism graduate students by a joint team from Citizen Clinic and the UC Berkeley School of Journalism during Fall 2020. In this course, student-journalists learned to safely and skillfully investigate extremist groups across the political spectrum, allowing them to produce and publish narrative news stories that reflect entrepreneurial reporting

58 Henrichsen, "Breaking Through" 334.
59 See, for example, Posetti.
60 Henrichsen, "Breaking Through" 342.
61 Henrichsen, "Breaking Through" 342.

and reveal new levels of understanding about these extremist groups, how their ideologies operate, and what their intentions are. In parallel, Clinic staff taught the students how to apply dynamic risk assessment skills for story development and production, as well as how to successfully integrate context and story-appropriate security practices into the reporting workflow. Students gained a unique ability to practice open source investigation techniques for story ideas, information verification, and background research while keeping themselves and their stories secure. Effective online security guides should also dangle this "carrot" in front of journalists while informing them about how to improve their online security: there is a dual purpose in nearly every security measure.

CATEGORY	METRIC
Strengthening the Fourth Estate	To what extent does the material help journalists carry out their role as monitor/watchdog, protector, or skeptic?

A final persuasive benefit for improving journalistic security is dependent on all the others: namely, adopting appropriate security measures and practices helps journalists carry out their vital role as watchdog, protector, and skeptic in society.[62] I assessed whether each guide, even at a high level, helps move the needle in this direction. For example, the guide might help make the journalist's accounts or device more secure, which enables them to confidently do the difficult work of investigating powerful targets. And when journalists are educated about security in a contextually appropriate way, they also gain insights about investigatory techniques that enable them to get visibility into more information. These are effectively two sides of the same coin: journalists investigating stories that the powerful do not want to be told need to have strong baseline security for themselves and their families, and they need to be armed with investigatory techniques that will help bring those stories to light.

I scored each security guide under these qualitative categories, using a numbered scale (on a scale from 1–5, with 1 being "not at all," and 5 being "extremely helpful") for each category. The highest possible score is 60. All of the data and scores are available to view at https://sites.google.com/view/journosec-guides/home.

62 Henrichsen, "Breaking Through" 342.

Findings

QUANTITATIVE FINDINGS

TABLE 3.

THE TOP 10 MOST FREQUENTLY MENTIONED ADVICE IMPERATIVES IN SECURITY GUIDES FOR JOURNALISTS:

1. Use multi-factor authentication.
2. Use Tor.
3. Use a password manager.
4. Create strong passwords. / Use Signal. (tied)
5. Back-up data from your mobile device or laptop regularly and in an encrypted fashion.
6. Don't re-use passwords.
7. Apply system and software updates.
8. Use passphrases.
9. Check for https:// in the browser.
10. Enable full-disk encryption.

Table 3 lists the advice imperatives that were most frequently mentioned across the 33 security guides analyzed. As detailed in Table 4, we compared this set of advice against lists from general (not journalist-directed) security advice evaluated by other researchers.

TABLE 4. SIDE-BY-SIDE TOP-TEN LISTS OF ADVICE IMPERATIVES FOUND IN SECURITY GUIDES FOR JOURNALISTS AND SECURITY GUIDES AND ADVICE FOR A GENERAL AUDIENCE.

Ranking based on frequency	Security guides for journalists	Security guides and advice for general audience		
	This paper: based on 33 guides	Redmiles et al.[63]: based on 1,264 guides	Busse et al.[64]: based on 75 security experts	Reeder et al.[65]: based on 231 security experts
1	Use multi-factor authentication	Use unique passwords for different accounts	Update system	Keep systems and software up to date
2	Use Tor	Update devices	Use unique passwords	Use unique passwords

63 Redmiles et al. research data repository.
64 Busse et al. 6.
65 Reeder et al. 61.

3	Use a password manager	Use anti-malware software	Use 2-factor authentication	Use strong passwords
4	Create strong passwords	Scan attachments you open for viruses	Use strong passwords	Use multifactor authentication
5	*~tied with~* Use Signal	Use different passwords	Use password manager	Use antivirus software
6	Back-up data from your mobile device or laptop regularly and in an encrypted fashion	Encourage others to use strong passwords	Check if https://	Use a password manager
7	Don't re-use passwords	Not tell anyone your passwords, even IT	Don't share info	Use HTTPS
8	Apply system and software updates	Use end-to-end encryption for communication	Use antivirus software	Use only software from trusted sources
9	Use passphrases	Remember your passwords	Use Linux	Use automatic updates
10	Check for https:// in the browser	Keep passwords safe if written down	Use verified software	Be careful/think before you click
	Enable full-disk encryption			

Table 5 shows that only two of the advice imperatives in guides for journalists are universally cited by each of the lists: "don't re-use passwords" and "apply system and software updates." These are two important and uncontroversial pieces of advice for any end-user, regardless of profession. Five of the advice imperatives were also mentioned in three of the lists. However, five of the top ten pieces of advice compiled from guides for journalists are not present at all in any of the other lists. In fact, each list in the table contains significant pieces of advice that are unique to that list. This finding aligns with prior research in the field: even "experts" do not agree on what the most important pieces of advice are for end-users.[66] Given this lack of consistency among experts, one might imagine that journalists and non-journalists alike are not sure where to start when they seek to improve their online security.

66 See, for example, Redmiles et al. 90: "We find little evidence that experts are any better off than end-users on the subject of security advice: experts identify 118 pieces of security advice as being among the top 5 things they would recommend to a user, consider 89% of the 374 pieces of advice to be useful, and struggle with internal consistency and alignment with the latest guidelines."

TABLE 5. MEASUREMENT OF CONSISTENCY AMONG ELEMENTS OF TOP-10 LISTS OF ADVICE IMPERATIVES.

ADVICE IMPERATIVES THAT APPEAR IN ***ALL FOUR*** TOP-10 ADVICE LISTS:

Don't re-use passwords / use unique passwords for each account
Apply system and software updates

ADVICE IMPERATIVES THAT APPEAR IN ***THREE OUT OF THE FOUR*** TOP-10 ADVICE LISTS:

Use a password manager
Create strong passwords
Check for https:// in the browser
Use anti-malware software / use antivirus software
Use multifactor authentication

ADVICE IMPERATIVES THAT APPEAR IN ***TWO OUT OF THE FOUR*** TOP-10 ADVICE LISTS:

none

ADVICE IMPERATIVES THAT APPEAR IN ONLY ***ONE OUT OF THE FOUR*** TOP-10 ADVICE LISTS:

Use Tor
Use Signal
Back-up data from your mobile device or laptop regularly and in an encrypted fashion
Use passphrases
Enable full-disk encryption
Scan attachments you open for viruses
Encourage others to use strong passwords
Not tell anyone your passwords, even IT
Use end-to-end encryption for communication
Remember your passwords
Keep passwords safe if written down
Don't share info
Use Linux
Use verified software
Use only software from trusted sources
Use automatic updates
Be careful/think before you click

While the advice in most of the security guides for journalists is internally consistent, there were inconsistencies among the 33 guides surveyed. Here are some of the significant inconsistencies found:

- Use removable media (e.g., a USB stick) for storage or boot. / Configure your computer not to allow booting from removable media.
- Do not use biometric authentication. / Maybe use biometric authentication? We're not sure.
- Automatically back-up data from your phone or laptop to the cloud. / Do not use automatic back-up to the cloud. (Similarly: Enable auto-updates. / Disable auto-updates.)
- Don't use cloud storage at all. / Do use cloud storage.
- Do a risk assessment. / Do threat modeling. (Example of inconsistent language to cover the same concept.)
- Use a password manager. / Don't use the browser's password manager.
- Don't use free software (context: VPNs). / Use free software (context: antivirus software).

At a high level, the top ten advice imperatives in security guides for journalists are prudent steps for any end-user to take (with the possible exception of Tor, which has a more limited use case for most users). Most of the top advice imperatives are general in nature, with only three specific tool recommendations (Tor, Linux, and Signal). This is noteworthy given the preponderance of tool recommendations overall: of the 297 advice imperatives that we extracted from the security guides for journalists, 129 were recommendations to use specific tools, or warnings *not* to use a specific tool. This large number of recommendations may be overwhelming, yet tools are critical for journalists and their workflow. As Henrichsen notes,

> [I]nformation security technologies are utilized in the external and internal spaces of newsrooms and thus could be articulated as interstitial actants. The positioning of information security technologies as interstitial technological actants that glide between the internal and external needs of a news organization suggests that they could be considered as an emerging form of "newsware" (Ananny 2013) and ultimately connected to cultural norms and practices of journalists. Examples of information security technologies include tools that help to protect data in transit such as the encrypted application, Signal.[67]

67 Henrichsen, "Breaking Through" 331.

Unfortunately, the guides do not devote much space to the "cultural norms and practices of journalists." A stand-out exception is Martin Shelton's Medium piece, "How to Lose Friends and Anger Journalists with PGP."[68] Shelton investigates why journalists might be interested in PGP ("Pretty Good Encryption," an encryption system) to secure their communications, and also why it may not be appropriate, given the way journalists work: "PGP opens the door to new conversations, but often, it also makes real work harder than it needs to be, and that makes journalists angry." The vast majority of security guides for journalists do not consider how the recommended tools might be integrated successfully into a journalist's time-pressured workflow.

QUALITATIVE FINDINGS

FOSS advocacy: Of the 33 guides surveyed, only six advocated for the use of open source software. As noted in the previous section, we included this category to assess whether open source software is a technical topic that security guides designed for journalists explain. Of the six guides that recommended FOSS, one caveated their advice by saying that the user must "verify the origin" of the FOSS, and they gave advice on how one might go about doing that.[69] As noted in the previous section, just because an app is FOSS does not inherently make it more secure. However, most guides that mention FOSS take increased security at face value—for example, one guide stated, "To increase confidence that your operating system does not have potential surveillance 'backdoors', it should be 'open source'."[70] One guide even went so far as to say, "Given the fact that there have been multiple vulnerabilities discovered in closed-source iOS apps (Snapchat as the most public example as of the time of writing), we do not suggest using or recommending these to users."[71] There have been "multiple vulnerabilities" reported in FOSS, too[72]—and, as with COVID-19, a lack of testing (researchers examining code and publishing reports) does not mean there is a lack of infection (vulnerabilities).

Cultural relevance: One of the security guides makes a point that is inadvertently a good analogy for the cultural environment: earthquakes.

68 Shelton.
69 Holmes.
70 PEN America.
71 Aryal and Jones 109.
72 See, for example, Coker.

> It is important to distinguish between what might happen and the probability it may happen. For instance, there is a threat that your building might collapse, but the risk of this happening is far greater in San Francisco (where earthquakes are common) than in Stockholm (where they are not).[73]

If we think about the journalist's context the same way we think about seismic zones, then we might say, there is a threat that your communications with a source might be intercepted by a government actor, but the risk of this happening is far greater in certain countries (where government surveillance of journalists is common) than in others (where it is less common). The overwhelming majority of security guides for journalists do not consider cultural relevance at all. One guide did refer to the context of gender norms in some countries, advising women reporters to dress modestly.[74]

Racial equity: Only one guide out of 33 came close to explicitly recognizing race as part of the context of journalism and security, advising readers to ask themselves before entering the field (emphasis added), "Do I know enough about the place where I am going? In particular, am I aware of how they behave *toward women, toward different social or ethnic groups*, and so on?"[75] A journalist of color may face greater risk depending on the story or beat they are covering, and that risk assessment may prompt the adoption of certain or additional security measures. Failure to do so may mean a range of consequences, from online harassment to physical harm.[76]

Role of sources: Six out of the 33 guides were rated 4 or 5 for giving due consideration to the role of sources and how they influence journalistic security. Here is a good example: "Each conversation is only as secure as the most insecure member of the conversation. Signal is a tool that has good options to protect both sides, but if a journalist is using Signal with a source who doesn't have a secure passcode or has left message previews exposed on their lock screen, the conversation may still be exposed. Similarly, the journalist should take as many steps and precautions a[s] possible to protect their sources by encouraging their sources to read guides on using Signal."[77] Fourteen of the guides recommend the use of Signal, but this is the only one that

73 Electronic Frontier Foundation.

74 Reporters Without Borders, "Safety Guide" 47.

75 Reporters Without Borders, "Safety Guide" 16.

76 "Seeing reporters physically harmed is jarring. Yet every day journalists face digital threats that can be devastating and drive away talent from the industry. Digital harassment is intensifying as tensions between political and social groups accelerate and hostility toward the press increases. Studies show women and journalists of color are more likely to be at the receiving end of abuse." Masullo and Supple.

77 OpenNews et al.

devotes particular attention to it in connection with sources, recognizing that one is still reliant on whatever security configuration a source has set up in their instance of Signal.

Risk assessment: A large number of security guides completely ignore risk assessments (or threat modeling, to use the security industry term). Some mention them, but not in a prioritized way that makes clear that risk assessment comes before tool selection. One guide covered risk assessment in the physical world comprehensively, but made only passing mention of its counterpart in the online world.[78] One very popular guide provided an extremely simplified generic threat modeling tutorial, with not a word devoted to journalists in particular. This is probably the most serious gap in security guides and training: the lack of prioritization given to the critical task of risk assessment, and for journalists, how to integrate assessment into one's everyday workflow to dynamically respond as stories and beats develop.

Personal protection: I concluded that most of the guides reviewed would improve a journalist's physical security, because of the interconnected nature of security between on- and offline worlds. In most cases, this was not an intentional effect as guides generally did not take a holistic approach to journalistic security.

Story investigation: Only nine of the 33 guides provide some tips and techniques that, if adopted, would bolster the investigatory skills of the journalist and enable them to cover more high-risk targets and beats. Henrichsen suggests that security guides and training for journalists would gain higher levels of adoption if "getting the story" was used as a "point of entry for persuading journalists to adopt information security practices."[79]

Strengthening the Fourth Estate: I graded this category generously, taking the tack that a journalist's adoption of any security measure covered in a guide would by definition (however small in effect) strengthen the Fourth Estate by making that journalist less vulnerable to digital attacks and mishaps.

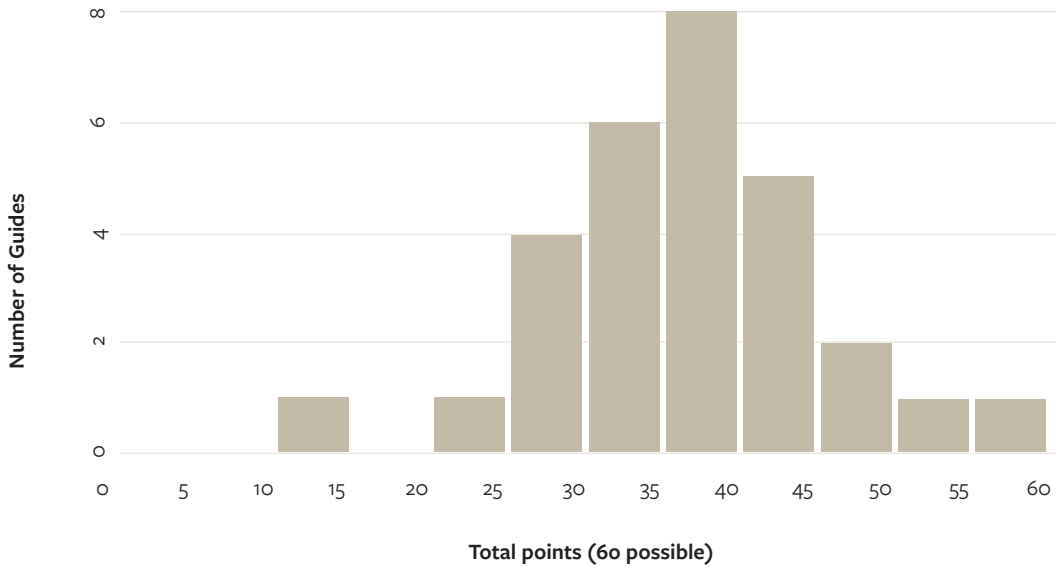
Most of the qualitative categories used a numbered score, between one and five. The highest score possible is 60. Table 5 shows the scoring spread, with most guides ranging between

78 Smyth, et al.

79 Henrichsen, "Breaking Through" 342.

30–45. While no guide received the highest possible score of 60, a couple of them exceeded 50. The highest scoring guide shines because it is the result of a collaboration among the journalist, tech, and security communities, providing contextually informed, practical advice.

TABLE 6. HISTOGRAM OF QUALITATIVE CRITERIA SCORES (60 POSSIBLE)



GENERAL OBSERVATIONS ABOUT ADVICE

It's hard to keep advice up to date. Many guides and articles are published and never revised by their authors. Over time, some recommended security measures may no longer be necessary since they may happen by default: e.g., full disk encryption on iOS and Android phones, or automatic malware/phishing detection on browsers and email services. Another consequence of a failure to keep a guide current is that features and functionality of products and services change over time, and if the guide is not updated, its content becomes stale: for example, several sites tell the reader to look for the padlock icon in the browser to determine whether a browser session is secure. However, Chrome began eliminating the padlock icon in 2018.[80]

Of the 207 tools that the guides recommend by name, only five are deprecated or no longer available or supported. That is somewhat surprising, considering there is no indication in most of the guides that they are reviewed and revised on a regular basis.

80 Schecter.

Some guides contain advice that is actively harmful. For example, one guide recommends that journalists disable auto-updates of apps or services. Most security professionals recommend that users enable auto-updates, specifically to ensure that the latest security patches are installed.[81]

Passwords and authentication are the most popular topic. Nearly every guide agrees that journalists need to use strong and unique passwords for each account, and they need to store those passwords in a password manager. There is a lack of agreement, however, on what constitutes "strong." Anywhere between six to sixteen characters is recommended.

Some self-contradicting, confusing, and downright harmful advice is found in these guides. This is one example:

> You can keep sensitive information off of your computer by storing it on a USB memory stick or portable hard drive. However, such devices are typically even more vulnerable than computers to loss and confiscation, so carrying around sensitive, unencrypted information on them is usually a very bad idea.

The author notes that this is "a very bad idea," but still suggests that you can do it anyway. For journalists pressed for time who have an ethical obligation to protect their data and sources, this kind of narrative is confusing and wasteful and could contribute to a journalist concluding that there are no worthwhile security measures.

Good advice is rarely a punchy soundbite. It is easy to issue a mandate like "use Signal," but it is difficult to communicate the nuanced assessment and considerations that go into most effective security measures. Here are a couple examples of good advice that would not fit on a bumper sticker:

- "The tool that you use should be dictated by the preference and situation(s) of the people that you need to communicate with and the country you are in. Always speak with your sources using the most secure method possible and be informed about who makes the tool you are using."[82]
- "Risks should be reassessed on a frequent basis as conditions change."[83]

81 Barrett.

82 Rory Peck Trust, "Encryption."

83 Smyth, "Assessing and Responding to Risk."

Challenges in Measurement

If we view online security practices as "innovations" for journalists (that is, "an idea, practice, or object that is perceived as new by an individual"[84]), then measuring the efficacy of security guides (or training) for journalists is difficult for three reasons.

First, the *consequences* of security guides and training are difficult to measure, regardless of whether the audience is made up of journalists or a more general group. Individuals using an innovation—in this case of this paper, journalists learning how to stay secure online—are often not fully aware of all the consequences of adoption.[85] One method commonly used to assess the efficacy of training is surveys. At Citizen Clinic, we have used surveys to try to determine the extent to which security measures have been adopted by an audience after training, but relying on the reports of survey respondents usually means one must draw conclusions from incomplete responses. For a guide published for the anonymous reading public on the internet, the challenge of determining efficacy is even greater as the audience is dispersed and in most cases unidentifiable. To counter this effect, we recommend that future researchers:

- Avoid direct questioning about security in order to minimize inaccurate responses. Instead, ask questions that incorporate the context in which the respondent operates (for a journalist, this could be the field or the newsroom, for example).
- Pursue indirect measurement: after receiving training or reading a guide, inquire whether the journalist was able to chase riskier stories because of their new skills and capabilities in security, rather than asking what they have done to improve their security.

Second, cultural relativism clouds perception. Rogers provides this caution when trying to perceive the consequences of a new practice:

> Cultural relativism poses problems for the measurement of consequences. Data about the results of an externally introduced innovation that are gathered from clients, change agents, or scientific observers, are subjectively flavored by their cultural beliefs. Consequences should be judged as to their functionality in terms of the user's culture, without imposing outsiders' normative beliefs about the needs of the client system.[86]

84 Rogers 12.
85 Rogers 441.
86 Rogers 441.

A security guide's author introduces readers (journalists) to security-related innovations, so the author has an inherent "cultural belief" in the usefulness of such innovations. Evaluation should be based on the security methods' functionality in terms of the journalist's culture and work environment—without imposing the author's normative beliefs about what that journalist or news organization needs. Security guides written by "security experts" often take the usefulness of their advice for granted, without consideration of the reader's context. As a result, guides spend more time discussing the details of end-to-end encryption than how a journalist might use end-to-end encryption in a particular situation to mitigate a particular risk.

The best guides take into consideration the milieu of the reader. The highest-scoring guides in our analysis (in terms of qualitative criteria) were published by authors or organizations with direct knowledge of how journalists work and the culture of news organizations.

Third, it is hard to separate consequences and tie them to specific causes. Effects of an innovation are difficult to determine in a precise manner, and, as Rogers noted, ". . . many important consequences are unanticipated and indirect."[87] The field of journalism is changing rapidly, in large part due to the impact of technological innovations such as social media and other online platforms.[88] To safely function online, and to be competitive in the media industry, journalists must adopt and adapt to technology in a secure fashion. However, it is challenging to predict how technology will evolve, and what security and online investigatory practices journalists will need to adopt in order to thrive. Rather than a one-time survey or, more likely, no analysis at all in the case of online guides, future research should consider formulating a case study or other sort of extended observation of journalists or news organizations over time, to truly and accurately understand the effects of security innovations.[89]

87 Rogers 442.

88 See, e.g., this article from the year 2000, which boldly predicted: "hand-sized reading devices will enable you to read/watch/hear media content any place you like." Regan.

89 "Extended observation over time, or an in-depth case study, are usually utilized to study consequences . . . the usual one-shot survey methods are inappropriate for investigating the effects of innovations." Rogers 440.

Recommendations

In short, prospective publishers of online security guides for journalists should think long and hard before posting advice on the internet. The internet is rife with such guides. There is too much advice out there, and most of it is presented in a way that is difficult to keep up to date and difficult for readers to understand how to prioritize what to do.

Guides like *Consumer Reports*' Security Planner[90] are effective partly because they take the reader's environment, assets, and protection goals and concerns into account before dispensing advice. A site like the Digital First Aid Kit[91] is effective because it addresses specific fact patterns and recommends mitigations for threats that have already occurred. Most guides, though, do not prioritize their content in any way, providing no path for a time-pressured journalist to follow to improve their security in an efficient way. Many are assemblages of otherwise unconnected articles on digital security, with no overarching path or logic. And without an understanding of risk, any reader will likely find it difficult to decide which advice imperatives to pursue from an assemblage configuration.

Of course, there is no question that these general recommendations given by other researchers are sound. To reiterate, any future guides developed should aim to provide advice that is:

- Effective: good advice should make a positive difference
- Actionable: good advice should be easy to carry out with the least amount of interference in the user's workflow
- Consistent: good advice should not be confusing or contradictory
- Concise: good advice should be clear and brief

Based on the review described herein, this paper contends that the best guides have certain additional characteristics that help make them more effective, as we shared in the previous section. The review also shows that the popular guides are not also consistently the highest scoring in terms of the qualitative criteria.

The key recommendations for security guides based on this analysis are:

90 See https://securityplanner.consumerreports.org/.

91 See https://digitalfirstaid.org/en/index.html.

1. **Always start with risk.** Help the journalist understand and assess the risk of their story or beat. Only then will the reader-journalist be receptive and curious about the tool or practice that is appropriate given their risk assessment.

2. **Integrate security practice with the journalist's workflow.** Journalists will allow only so much friction in their workflow, given the unceasing time pressure of publication. If they first recognize the threat, appropriately measure the risk, and choose a tool or practice they can work with, the chances of long-term success in maintaining strong security will rise significantly.

3. **Security as a competitive advantage.** Life happens online. Journalists get attacked and harassed online, but they also find breaking stories online, too. The journalist who knows how to mine the public internet for stories will have a competitive advantage over those who do not. The journalist who has secured their accounts and devices will be empowered to safely explore the darker corners of the internet to extract the information needed to tell the stories that help maintain democracy and freedom in society.

4. **Newsrooms and journalism schools should integrate security education into their programs.** Websites and PDFs posted on the internet are pieces of static content designed for an individual to read as a solitary experience. The authors of security guides publicly posted on the internet probably do not know how their work is being received and whether their advice is being implemented (unless a reader is motivated enough to give them feedback). There are two environments where security education for journalists would be ideal: the newsroom and the classroom. It has been observed that, in most newsrooms and journalism schools today, security is still an afterthought (if it is thought of at all). This observation from a survey of journalism schools in 2018 resonates even more loudly in today's hostile environment for journalists:

> Once considered the exclusive concern of national security reporters, basic digital security competence is now essential for all journalists. Online mobs try to silence writers—especially women and people of color—by finding and leaking their personal information online; criminals lock down publishers' systems and try to extort ransoms; metadata can leave breadcrumbs back to vulnerable sources; and one misguided click or weak password could let intruders into a whole news organization's system. These days, bad security habits could betray your sources, or the sources of the reporter sitting next to you.[92]

92 Oliver.

This survey of journalism programs in the United States and Canada found that only half of the schools that responded to the survey "offered security training, and less than a quarter make that training mandatory. Among programs that have training, the majority devote less than two hours to the subject."[93] News organizations are not doing much better. A 2020 report described the culture of security in newsrooms as "nascent."[94] Imagine how much more effective journalists could be if they had institutional support for their online security and if journalism schools graduated students with the skills to protect themselves and their stories, as well as the investigative techniques to get the stories.

93 Oliver.

94 Henrichsen, "The Rise" Executive Summary, 80.

Conclusion

In addition to the challenges of measuring the efficacy and impact of security guides for journalists discussed in the previous section, we observed in our review of guides that the advice of security professionals and guides is not always consistent. This finding is in line with the conclusions of other researchers who have reviewed security advice for a general audience:

- "Past research on security advice and users' security behaviors suggests that there's an opportunity for advice to change behavior for the better but also a need to limit, prioritize, and better communicate the advice."[95] Reeder also recommends that advice "should be informed by actual data about attacks, compromises, and breaches"[96]—in other words, advice should be contextually informed and risk-appropriate for the intended audience.
- "Our results suggest a crisis of advice prioritization. The majority of advice is perceived by the most users to be at least somewhat actionable, and somewhat comprehensible. Yet, both users and experts struggle to prioritize this advice."[97]

This paper's advice census made similar findings: most advice is indeed somewhat actionable and somewhat comprehensible. But it is not presented in a way that will give time-pressed journalists a clear understanding of what measures should take priority.

This paper posits that one reason journalists are not taking actions to protect themselves online is that there is too much security advice for journalists out there, most presented in a way that is challenging to keep up-to-date and difficult for journalist-readers to understand how to prioritize what to do. Most of the guides reviewed do not account for journalists' workflow and environment: journalists are deadline-driven, and in a 24/7 news culture, time pressures are significant. Journalists also operate in an increasingly hostile environment, even in countries with democratic governments with some historical guarantees of freedom of the press and rule of law.

The digital age provides immense opportunities for investigative journalism, but it also offers a thousand ways in which journalists can get trolled, threatened, and harmed. Security education for journalists must be contextually-informed, prioritized, and actionable to be effective and to facilitate journalists' critical role in democratic society. That education should happen across

95 Reeder et al. 56.
96 Reeder et al. 63.
97 Redmiles et al. 89.

multiple venues—online and offline—and address both freelance and affiliated journalists: security education should be integrated into the curricula of journalism schools, and adopted by newsrooms as standard practice. Publicly available guides can be effective and important for journalists, particularly for freelance journalists not affiliated with an organization, if they meet the criteria proposed in this paper.

Acknowledgments

The author is grateful to Randy Cantz, UC Berkeley, History, 2021, for assistance with the advice census. The review and feedback provided by these individuals was invaluable: Jennifer Henrichsen, Visiting Fellow at Yale's Information Society Project at Yale Law School and a PhD candidate at the Annenberg School for Communication at the University of Pennsylvania; Siena Anstis, senior legal advisor, Citizen Lab, University of Toronto; and Kathy Berdan, editor at Pioneer Press, St. Paul, Minnesota. The author thanks colleague Steve Trush, Citizen Clinic, UC Berkeley, for review and for assistance with data visualization. This paper was made possible with support from Craig Newmark Philanthropies.

Works Cited

Aryal, Manisha and Dylan Jones. "Safer Journo: Digital Security Resources for Media Trainers." Internews, 2014, https://www.internews.org/sites/default/files/resources/SaferJournoGuide_2014-03-21.pdf.

Barrett, Brian. "Turn On Auto-Updates Everywhere You Can." *Wired*, 8 March 2019, https://www.wired.com/story/turn-on-auto-updates-everywhere/.

Busse, Karoline, et al. "Replication: No One Can Hack My Mind Revisiting a Study on Expert and Non-Expert Security Practices and Advice." Proceedings of the Fifteenth Symposium on Usable Privacy and Security. 12-13 August 2019, www.usenix.org/conference/soups2019/presentation/busse.

Citizen Clinic. "PESTLE-M Worksheet." Citizen Clinic Cybersecurity Education Center, 20 April 2020, www.citizenclinic.io/Clinic_Curriculum/Modules/Contextual_Research/PESTLE-M_Worksheet/.

Citizen Clinic. "Threat Modeling Overview." Citizen Clinic Cybersecurity Education Center, 17 November 2020, www.citizenclinic.io/Clinic_Curriculum/Modules/Threat_Modeling/Threat_Modeling/.

Coker, James. "Open Source Software Vulnerabilities Increased By 130% in 2019." InfoSecurity Group, 8 June 2020, https://www.infosecurity-magazine.com/news/open-source-vulnerabilities/.

Committee to Protect Journalists. "The Trump Administration and the Media." 16 April 2020, cpj.org/reports/2020/04/trump-media-attacks-credibility-leaks/.

Downie, Jr., Leonard and Sara Rafsky. "The Obama Administration and the Press." Committee to Protect Journalists, 10 October 2013, cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911/.

Duncan, Kat. "The Cohort: Newsrooms should protect staff against online harassment. Because they often don't, there's JSafe." *Poynter*, 24 March 2020, www.poynter.org/business-work/2020/newsrooms-should-protect-staff-against-online-harassment-because-they-often-dont-theres-jsafe/.

Electronic Frontier Foundation. "Your Security Plan." Surveillance Self-Defense, 10 January 2019, https://ssd.eff.org/en/module/your-security-plan.

Free and open source software. (2020, November 13). In *Wikipedia.* en.wikipedia.org/wiki/Free_and_open-source_software.

Glaser, April. "13 security tips for journalists covering hate online." *Journalist's Resource*, 15 May 2020, journalistsresource.org/tip-sheets/reporting/13-security-tips-journalists-hate-online/.

Glaser, April. "It Just Got a Lot Harder for the Proud Boys to Sell Their Merch Online." *Slate Magazine*, 7 February 2019, slate.com/technology/2019/02/proud-boys-1776-shop-paypal-square-chase-removed.html.

Halliki Harro-Loit & Beate Josephi. "Journalists' Perception of Time Pressure: A Global Perspective," *Journalism Practice*, 2020, 14:4, 395–411, DOI: 10.1080/17512786.2019.1623710.

Hasso Plattner Institute of Design at Stanford University. "Critical Lens Protocol." 2020, dschool.stanford.edu/resources/criticallens.

Henrichsen, Jennifer R. "Breaking Through the Ambivalence: Journalistic Responses to Information Security Technologies." *Digital Journalism*, 8:3, 328-346, 2020, DOI: 10.1080/21670811.2019.1653207.

Henrichsen, Jennifer R. "The Rise of the Security Champion: Beta-Testing Newsroom Security Cultures." Tow Center for Digital Journalism, Columbia University, 3 June 2020, DOI: 10.7916/d8-4enh-e398.

Herley, Cormac. "So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users." New Security Paradigms Workshop, 2009, www.nspw.org/papers/2009/nspw2009-herley.pdf.

Holcomb, Jesse, and Amy Mitchell. "Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior." *Pew Research Center*, 5 February 2015, www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/.

Holmes, Harlo. "Verifying open source software." Freedom of the Press Foundation, 6 April 2020, https://freedom.press/training/verifying-open-source-software/.

Horsley, William. "OSCE Safety of Journalists Guidebook," Office of the OSCE Representative on Freedom of the Media, 2012, www.osce.org/files/f/documents/d/7/85777.pdf.

International News Safety Institute. "Staying Safe Online," https://newssafety.org/safety/advisories/staying-safe-online/.

LaForme, Ren. "Journalists, it's unethical to ignore your online security." *Poynter*, 23 April 2018, www.poynter.org/tech-tools/2018/journalists-its-unethical-to-ignore-your-online-security-2/.

Machill, Marcel Machill and Markus Beiler. "The Importance of the Internet for Journalistic Research," *Journalism Studies*, 25 February 2009, 10:2, 178-203, DOI: 10.1080/14616700802337768.

Masullo, Gina and Carolyn McGourty Supple. "News leaders and tech platforms must safeguard journalists from digital harassment to ensure press freedom." Poynter, 8 July 2020, www.poynter.org/ethics-trust/2020/news-leaders-and-tech-platforms-must-safeguard-journalists-from-digital-harassment-to-ensure-press-freedom/.

McCudden, Kirstin. "Our September 2020 Newsletter." U.S. Press Freedom Tracker, Freedom of the Press Foundation, 1 September 2020, pressfreedomtracker.us/blog/our-september-2020-newsletter/.

McGregor, Susan and Elizabeth Watkins. "'Security by Obscurity': Journalists' Mental Models of Information Security." International Symposium on Online Journalism, January 2016, www.researchgate.net/publication/316609881_'Security_by_Obscurity'_Journalists'_Mental_Models_of_Information_Security.

Oliver, Joshua. "Journalism schools still behind on cybersecurity training, new survey finds." *Columbia Journalism Review,* 8 January 2018, www.cjr.org/innovations/journalism-schools-behind-cybersecurity.php.

OpenNews et al. "Setting up Signal." The Field Guide to Security Training in the Newsroom, 6 Jun 2017, https://securitytraining.opennews.org/en/latest/Chapter02-03-Setting-Up-Signal.html?highlight=source#lesson-plan.

Owen, Diana. "ICFJ SURVEY: The State of Technology in Global Newsrooms." International Center for Journalists, 2018, www.icfj.org/sites/default/files/2018-04/ICFJTechSurveyFINAL.pdf.

PEN America. "Online Harassment Field Manual." https://onlineharassmentfieldmanual.pen.org/.

Posetti, Julie. "Online Violence: The New Front Line for Women Journalists." International Center for Journalists, 24 September 2020, www.icfj.org/news/online-violence-new-front-line-women-journalists.

Redmiles, Elissa, et al. "A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web," Proceedings of the 29th USENIX Security Symposium, 12-14 August 2020, www.usenix.org/conference/usenixsecurity20/presentation/redmiles. Research data repository for this paper: https://securityadvice.cs.umd.edu/expert-ranking.html.

Reeder, Robert, et al. "152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users." *IEEE Security and Privacy*, 2017, research.google/pubs/pub46306/.

Regan, Tom. "Technology Is Changing Journalism." *NiemanReports*, 15 December 2000, niemanreports.org/articles/technology-is-changing-journalism/.

Reporters Without Borders. "Online Harassment of Journalists: Attack of the Trolls," 25 July 2018, rsf.org/sites/default/files/rsf_report_on_online_harassment.pdf.

Reporters Without Borders. "Safety Guide for Journalists," 2015, https://rsf.org/sites/default/files/2015-rsf-safety-guide-for-journalists.pdf.

Rogers, Everett M. *Diffusion of Innovations*. Simon & Schuster, 5th ed.

Rory Peck Trust. "Digital Security Guide," https://rorypecktrust.org/freelance-resources/digital-security/.

Satter, Raphael, et al. "Russian hackers hunted journalists in years-long campaign." *Associated Press*, 22 December 2017, apnews.com/article/c3b26c647e794073b7626befa146caad.

Schecter, Emily. "Evolving Chrome's security indicators." *Chromium Blog*, 17 May 2018, blog.chromium.org/2018/05/evolving-chromes-security-indicators.html.

Shelton, Martin. "How to Lose Friends and Anger Journalists with PGP." *Medium*, 14 July 2017, https://mshelton.medium.com/how-to-lose-friends-and-anger-journalists-with-pgp-b5b6d078a315.

Signal Technology Foundation. Signal. GitHub, 2020, github.com/signalapp.

Smyth, Frank, et al. "CPJ Journalist Security Guide." Committee to Protect Journalists, 2012-2020, https://cpj.org/reports/2012/04/journalist-security-guide/.

Southern Poverty Law Center. "Proud Boys." Southern Poverty Law Center, www.splcenter.org/fighting-hate/extremist-files/group/proud-boys, accessed 20 November 2020.

Stewart, Camille. "Systemic Racism is a Cybersecurity Threat," Council on Foreign Relations, 16 June 2020, www.cfr.org/blog/systemic-racism-cybersecurity-threat.

Sullivan, Margaret. "Leak Investigations Are an Assault on the Press, and on Democracy, Too." *New York Times*, 14 May 2015, publiceditor.blogs.nytimes.com/2013/05/14/leak-investigations-are-an-assault-on-the-press-and-on-democracy-too/.

The Tor Project, Inc. Tor. Github, 2020, github.com/thetorproject.

Westcott, Lucy. "Journalist safety in the U.S., Canada." Committee to Protect Journalists, 2019, infogram.com/cpj-safety-survey-sept-2019-1hon25jdd3z06pe?live (infographic). Westcott, Lucy. "'The threats follow us home': Survey details risks for female journalists in U.S., Canada." Committee to Protect Journalists, 4 September 2019, cpj.org/2019/09/canada-usa-female-journalist-safety-online-harassment-survey/.

UNESCO. "Trends in the safety of journalists." World trends in freedom of expression and media development: global report 2017/2018, 2018, unesdoc.unesco.org/ark:/48223/pf0000261372.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley