TAKING THE PULSE OF HACKING:

A RISK BASIS FOR SECURITY RESEARCH

MARCH 2018

Table of Contents

Cover designed by: Timothy Hoagland

CENTER FOR
DEMOCRACY
& TECHNOLOGY

TAKING THE PULSE OF HACKING:
A Risk Basis for Security Research

March 2018

Authors: Joseph Lorenzo Hall (CDT), Stan Adams (CDT)

1 Introduction

Over the past thirty years, we have seen substantial growth in computing and networking to the extent that those two elements now occupy the prefix "cyber," anointing everything from cyberlaw to cybersecurity. We have also seen a natural growth in people interested in tinkering with these systems, from makers to security researchers to hackers, all finding ways to remix technologies, services, and social practices into new artifacts of our growing digital culture.

Since the first computer virus, the Morris Worm, there have been conflicts around what people should and should not do with computer and network technologies. Some of these conflicts remain in the technical realm with various parties fighting it out online, but other conflicts fall within the purview of the law. In the civil sense, aggrieved parties sue hackers for a perceived wrong, and in the criminal sense, prosecutors seek to hold someone responsible and criminally liable for wrongdoing in cyberspace.

Over the past three decades, the community that investigates vulnerabilities in computers and networks – the computer and information security research community – has grown. Beginning as a hobby of early computer scientists such as Cliff Stoll,[1] the security research community has become a well-defined industry element that seeks to help defend information systems and networks, and to discover and repair new weaknesses in systems that billions use everyday.[2]

We sought to study the interaction between the law, technology, and this community. Specifically, since security researchers tend to push into grey areas where the law is unclear, an understanding of the law's "chilling effects" (inhibition or discouragement) on security research has been a major concern of those who work in and with information security. We asked security researchers and hackers what factors affect the kinds of work they choose to engage in. We then distilled those interviews to reveal the various levels of risk that researchers

[1] Stoll, Cliff. *The cuckoo's egg: tracking a spy through the maze of computer espionage*. Simon and Schuster, (2005).
[2] Center for Democracy & Technology, *The Importance of Security Research: Four Case Studies* (2017) https://cdt.org/files/2017/12/2017-12-15-Importance-of-Security-Research.pdf.

associate with certain activities. We hope to update this “risk basis” as new activities in security research develop and existing practices become the norm.

The report consists of 5 sections. Section 2 of this report describes the methodology for the qualitative investigation we employed. Section 3 discusses findings from these interviews, focusing on laws such as the Digital Millennium Copyright Act (DMCA) and the Computer Fraud and Abuse Act (CFAA), as well as vulnerability disclosure and other community norms. In Section 4, we describe a risk basis, listing common activities discussed in our interviews and assessing to what extent certain methods of performing those activities are more or less risky. We provide concluding thoughts in Section 5.

2 Methodology

We used a qualitative methods research design to understand how security researchers decide whether to pursue or to avoid certain kinds of projects and activities. It can be difficult to probabilistically sample hackers and security researchers to gain insights from quantitative methods. With this in mind, we decided instead to dig deeply into the decisions they make through semi-structured qualitative interviews.

Using a “snowball” sampling strategy, we chose a few initial subjects who we believed, through our own experience with the security research and information security community, possessed particularly useful insight into chilling effects. At the same time, we asked our subjects not just about things they do or feel themselves, but also about the experiences of those in their immediate networks in order to capture chilling effects that might spread organically. At the end of each interview, we asked subjects to suggest others that they thought we should interview.[3] We interviewed a total of 20 subjects, trying to interview equal numbers of academic and independent researchers; we were limited by our capacity and diminishing returns on the scope and strength of information obtained from additional interviews.

Among the 20 security researchers we interviewed, half are employed by academic institutions. The other half are either employed by a private firm or work independently. Two are women and the overwhelming majority identified as white or European when we asked them about ethnicity. (Studying differences in chilling effects across gender and ethnicity is a very promising line of future work in this area.).

[3] The qualitative interview instrument we used in this study is attached in Appendix A.

Due to concerns about the potential legal ramifications of retaining the research data and the concomitant risks to our subjects,[4] we did not make video or audio recordings of the interviews. Instead we took extensive, real-time notes of responses to interview questions (all research materials have been securely destroyed before public release of this paper). Additionally, borrowing a technique from ethnographic methods, we reviewed the interview notes immediately after each interview to correct mistakes, expand shorthand, and add material discussed in the interview but omitted in the initial notes.

These interview notes were then analyzed using a lightweight form of grounded theory:[5] Two CDT staff independently reviewed the text of each set of notes, adding tags to text that noted common themes among the subjects' responses. We used these tags to write research memorandums on specific themes across the data set about the DMCA, CFAA, disclosure, and normative considerations.[6] We then re-read the interview notes and modified the memos to reflect additional insights gained from a second review.

The result is a non-representative view of the considerations that security researchers and hackers take into account throughout the course of their work.

2.1 Limitations

Naturally, there are important limitations to this work. Our qualitative results are not representative; as we lack a sampling method for the security research and information security communities that would yield generalizable quantitative results. This is undoubtedly a function of the diffuse nature of those communities. In addition to sampling difficulties that stymie quantitative work, we wanted richer data than quantitative methods can provide. Qualitative interviews allow us to deviate from the interview instrument, to probe more deeply in areas of particular interest, while providing a standard structure for comparison across interview subjects.

Given our interests in preventing the association of subjects' identities with our interview data, this report exercises caution when referring to subjects, preferring gender-neutral pronouns,

[4] Recent years have seen compelled production of research data by the US Federal Bureau of Investigation, which chills research into activities that may be of interest to federal law enforcement. *See* Joseph Cox, *Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds*, (Feb. 24, 2016) Motherboard, https://motherboard.vice.com/en_us/article/d7yp5a/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds.

[5] Urquhart, C., H. Lehmann, and M.D. Myers, "Putting The 'Theory' Back Into Grounded Theory: guidelines for grounded theory studies in information systems." *Information Systems Journal*, (2010). 20(4): p. 357-381.

[6] Some topics from our questionnaire, such as researchers' interactions with Institutional Review Boards did not evoke strong responses across the sample.

abstracting potentially identifying details, and omitting certain inherently revealing anecdotes or techniques.

3 Findings

With regard to the DMCA, the CFAA, vulnerability disclosure practices, and other community norms, our analysis of the interview responses reveal the following:

3.1 Digital Millennium Copyright Act

One provision of copyright law, Section 1201 of the DMCA, prohibits the circumvention of access controls protecting copyrighted material. This prohibition applies to all acts of circumvention, even where no copyright infringement occurs. Although the DMCA contains several purpose-based exemptions to the prohibition, including one for encryption research and one for security testing, the language of these exemptions makes their application to current research practices uncertain. For example, the statutory exemptions for both encryption research and security testing require considering non-exclusive lists of factors when determining one's eligibility for each exemption, but the statute gives no guidance for how to weigh these factors or what the threshold for eligibility is.[7]

Nearly half of the researchers interviewed mentioned the DMCA specifically as a source of legal risk. Some researchers listed the DMCA as a primary source of risk and noted its chilling effect on their project choices. In some cases, researchers avoided working with devices and systems protected by access controls to eliminate the legal risks stemming from the DMCA. Others were willing to accept the level of risk they perceived the DMCA posed. One researcher who had

[7] 17 U.S.C. §1201(g)(3)(3) Factors in determining exemption.— In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include— (A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security; (B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and (C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.; (j)(3) Factors in determining exemption.— In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include— (A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and (B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

done work involving a circumvention of access controls felt more comfortable performing circumventions when there was no media content, such as music or video, behind the access control. This risk preference was based on an observation that more DMCA case law arose from circumventions involving some form of entertainment content than where the copyrighted code was not related to digital media. Another researcher echoed this assessment, reporting a lower level of concern when circumventing access controls on manufactured products (without media content), and noting that this kind of research had become socially normalized.

This perception reflects a difference in the outcomes of Section 1201 cases based on the kinds of interests at stake. Courts have tended to read the statute more broadly where circumvention allowed access to digital media on the grounds that Section 1201 was intended to protect copyright interests.[8] In contrast, in cases involving circumvention to facilitate interoperability of manufactured products, courts have tended to read the statute more narrowly, giving less protection to interests unrelated to copyright, such as controlling a market for manufactured goods.[9] Therefore, research requiring circumventing an access control protecting digital media may pose a higher degree of legal risk than where no media content is involved.

At least one researcher reported receiving a letter threatening legal action under the DMCA. There have been several documented instances of researchers facing legal threats citing the DMCA.[10] In one case, a researcher was arrested and charged with DMCA violations.[11]

The researchers expressed varying degrees of knowledge about the DMCA and its application to security research. Specifically, subjects noted that cryptographic research projects and projects involving digital rights management technologies (DRM) were more heavily influenced by concerns about DMCA liability than other subject areas. Several indicated that they sought the advice of legal counsel any time they encountered, or thought they might encounter, access controls. In some cases, researchers consulted counsel out of concern for their own personal liability. Others sought legal advice out of concern for the potential legal and reputational effects on their employers or educational institutions. One subject advised student researchers to seek legal counsel on a project involving DRM and web-hosted video content. This level of risk avoidance may be appropriate given the relationships between student, teacher, and

[8] See *Universal City Studios, Inc. v. Eric Corley*, 273 F.3d 429 (2nd Cir. 2001); *MDY Industries, LLC v. Blizzard Entertainment, Inc. and Vivendi Games, Inc*., 629 F.3d 928 (9th Cir. 2010).

[9] *See Lexmark International, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004); *Chamberlain Group, Inc. v. Skylink Tech, Inc*., 381 F.3d 1178 (Fed. Cir. 2004); *MGE UPS Systems, Inc. v. GE Consumer and Industrial, Inc.*, 622 F.3d 361 (5th Cir. 2010). *See also* Alicia Hoffer, A Matter of Access: How Bypassing DRM Does Not Always Violate the DMCA, 7 Wash J.L. Tech. & Arts 13 (2011) http://digital.law.washington.edu/dspace-law/handle/1773.1/1049.

[10] Several instances of legal threats against researchers can be found at http://attrition.org/errata/legal_threats/.

[11] *United States v. Elcom, Ltd. and Dmitry Sklyarov*, 203 F.Supp.2d 1111 (N.D. Ca. 2002).

university; a professor should not knowingly expose all three parties to legal liability. More generally, seeking legal counsel may indicate areas where uncertainty about the law and potential liability overlap.

Most researchers mentioning the DMCA as a risk factor expressed certainty about their ability to identify when their work might implicate the DMCA. However, few were confident in their ability to determine what was permissible when the DMCA was clearly implicated or to assess the potential legal consequences of different projects. At least one commented specifically on the uncertainty of the DMCA, noting the chilling effects this uncertainty had on their consideration of DMCA-related work. By contrast, some subjects acknowledged that some of their past projects had almost certainly violated the statute. One researcher demonstrated an awareness of the DMCA's statutory exemption for security research, but an incomplete understanding of the conditions for eligibility. This subject's interpretation, that circumvention for "curiosity" is exempt so long as there is no infringement of copyright, is incorrect, but perhaps reflects a way to rationalize the tension between the letter of the law and the various judicial interpretations of the law's spirit.[12] Although the law prohibits circumvention outright, some judges have looked beyond the act of circumvention for evidence of copyright infringement.[13] The same researcher also expressed interest in DRM circumvention as a student project, but questioned how the law might view bypassing DRM for educational purposes.

3.2 Computer Fraud and Abuse Act

The CFAA prohibits accessing a "protected computer" without authorization or in a way that exceeds authorization.[14] Violating the CFAA can result in criminal penalties, including imprisonment, even where the defendant's actions resulted in no harm or financial loss.[15] Unfortunately, the judicial interpretations of this statute are both broad and inconsistent.[16]

[12] See above regarding differences between using 1201 to protect copyright interests versus non-copyright interests. *Supra*, n. 8,9.

[13] See, e.g., *Lexmark*, *supra,* n. 9.

[14] 18 U.S.C. §1030. A "protected computer" has come to mean any computer, including mobile devices, connected to an interstate network.

[15] 18 U.S.C. §1030(a)(2)(C), (c)(2)(A) "Whoever intentionally access a computer without authorization, or who exceeds authorized access, and thereby obtains information from any protected computer...shall be punished as provided in subsection (c) of this section. The punishment for an offense under subsection (a) or (b) of this section is, except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph

[16] The Second, Fourth, and Ninth Circuits interpret the statute's phrase "exceeding authorized access" narrowly, limiting it to instances of traditional hacking activity, which might include, among other activities, bypassing some kind of access control or stealing financial account data. (*United States v. Valle*, 807 F.3d 508 (2d Cir. 2015); *WEC Carolina Energy Solutions v. Miller*, 687 F.3d 199 (4th Cir. 2012); *United States v. Nosal*, 676 F.3d 854 (9th Cir.

Although originally written to protect federal government computers and some financial institutions, amendments and judicial precedent have expanded the scope of this law to include virtually all computers (including mobile devices) connected to the internet.[17] This inconsistency, combined with the practical realities of many research methods, creates uncertainty. Uncertainty potentially resulting in steep criminal penalties creates a significant chilling effect for researchers.

Half of the interview subjects reported the CFAA as a primary source of risk. Of those, more than half reported avoiding some or all types of research that might implicate the CFAA. One subject reported not being concerned with the CFAA at all because of their complete avoidance of all potential involvement with the statute (i.e., networked systems). Others were more specific about what kinds of methods they avoided to reduce or eliminate risk of liability under the CFAA. Three researchers noted that they avoided logging into, communicating with, or "working with" computers or servers that did not belong to them. One noted that logging into someone else's server was both illegal, based on their understanding of the CFAA, and also unnecessary or impractical for the purposes of their research. Another noted that the transition to service-oriented computing ("cloud computing") meant that many more computing applications happen over a network connection and, accordingly, significantly more research areas require access to someone else's computer, and that the legal risk of doing so was too great. This subject mentioned testing the security of a major social networking platform as an example of a project precluded by personal CFAA concerns. For these researchers, completely avoiding activities that might be seen as "accessing" is the most certain way to avoid liability under the CFAA.

Much of the uncertainty associated with the CFAA stems from the phrase "exceeds authorized access." This uncertainty has at least two elements: the limits of authorized access and the means by which those limits are set. What this means for researchers is that, when they wish to interface with another machine or system, it is not always clear what they can do. One researcher noted that some servers were configured in a way that essentially allowed unfettered public access, making it impossible to determine what kinds of access the server's

2012)), while the First, Fifth, Seventh, and Eleventh Circuits read the phrase more broadly, including using a computer for purposes prohibited in a terms of use agreement (*EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577 (1st Cir. 2001); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010)).

[17] *See Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc*., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000). *See also* H. Marshall Jarrett et al., *Prosecuting Computer Crimes*, at 4, U.S. Dept. of Justice, Computer Crimes and Intellectual Property Section (2015) ("In a nutshell, "protected computer" covers computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions").

owner intended.[18] One researcher reported trying to avoid implicating the CFAA while researching onboard vehicle diagnostic systems where the car was also connected to the manufacturer's servers because of uncertainty about the bounds of authorized access. One subject indicated uncertainty as to how the CFAA might apply to accessing malware hosts. Another noted that, in certain scanning exercises, there was no method by which operators could signal whether or not they authorized access to information on their systems. As a result, the researcher was forced to choose between not conducting the research or potentially running afoul of the CFAA. Although network scanning has, as one subject notes, become a standard practice, many researchers employ methods to make their web traffic readily identifiable to allow operators to send opt-out messages. Another subject noted preference for a method of scanning which results in obtaining zero data, thereby leaving that element of Section 1030(a)(2)(C) unsatisfied.

Even where access limits are expressed, such as through Terms of Service (TOS) or End User Licensing Agreements (EULAs), it may not be certain how much legal weight those limits carry.[19] For example, one subject noted uncertainty about whether the terms of a EULA accepted by a third party were binding. Although many acknowledged the uncertainty and the risk, the perceived degree of risk associated with a failure to comply with TOS or EULAs varied from subject to subject. Two subjects tried to avoid work involving user agreements, but indicated that they would stay within their bounds to avoid CFAA liability. Another reported reading TOS very carefully before proceeding with research, but noted the practical impossibility of doing so at scale, for example in an internet-wide network scan. Another researcher echoed this point, noting that TOS are not always machine-readable, which presents a practical issue for network scanning. This subject attempted to mitigate the risk of accidentally or unknowingly exceeding authorized access by designing scanning tools to look for common TOS text. One subject reported that TOS were not necessarily a deterrent, even where the project might require violating a term. However, the subject reported avoiding work in cases where TOS explicitly prohibited system analysis. By contrast, one researcher seemed unconcerned that TOS might

[18] Subject also noted a certain network management protocol (SNMP) presented problems in determining where authorized access ended because its configuration allowed access when the "community string" is set to "public," which is the factory default setting on devices with earlier versions of the protocol. See Paessler, *What is an "SNMP Community String"* , https://www.paessler.com/whatisansnmpcommunitystring. *See also* Deral Heiland, *Simple Network Management Protocol (SNMP) Best Practices*, Rapid7, (Jan. 27, 2016) https://blog.rapid7.com/2016/01/27/simple-network-management-protocol-snmp-best-practices/.

[19] For example, the Skype terms of use agreement says users may not "undertake, cause, permit or authorise the modification, creation of derivative works or improvements, translation, reverse engineering, decompiling, disassembling, decryption, emulation, hacking, discovery or attempted discovery of the source code or protocols of the Software or any part or features thereof (except to the extent permitted by law), Skype Terms of Use, 4.2(b) https://www.skype.com/en/legal/tou-connect/#1. See also note 16, *supra*.

create liability under the CFAA based on a perception of legal immunity derived from status as a scientist rather than a consumer.

One method of access was almost unanimously rejected by those we interviewed: using found or stolen credentials to access a system. Although this viewpoint was driven, in part, by ethical concerns, it also reflected an assessment that using credentials other than your own constituted unauthorized access or access exceeding authorization. There was some variation in terms of how far our subjects considered too far. One subject noted that using credentials to test for login success was acceptable so long as the connection was severed immediately after login. In their view, this stopped short of "accessing." Another indicated that trying to access a dummy account (created by the researcher) would be legally and ethically acceptable.

3.3 Disclosure

The process of vulnerability disclosure is a frequent part of the work of a security researcher. There is a long history of disclosure methods and disclosure can be very complicated, especially when multiple parties are involved on either side of the equation. When researchers discover flaws and vulnerabilities, they must choose what to do with the information. This decision may reflect a significant difference between so-called "black hat" and "white hat" hackers: black hats exploit (or threaten to exploit) the flaw or vulnerability for personal gain, but white hats hope to share the information in ways that will minimize the harms the flaw or vulnerability may cause. In most cases, this means sharing the information with the company or companies responsible for implementing a patch or mitigation method. In other cases, it may mean sharing the information with a larger set of actors, such as other members of the research community or the federal government. Researchers in other scenarios may find public disclosure to be the best way to mitigate damage by raising awareness of the flaw. In some of those cases, researchers use delayed public disclosure to incentivize a time-sensitive response from the company.[20]

From the perspective of vendors and manufacturers, public disclosure of flaws or vulnerabilities may pose risks of reputational harm and potential legal liability. Vendors may lack the resources or the incentive to develop and implement a patch or mitigation method, in which case

[20] Andi Wilson, Ross Schulman, Kevin Bankston, and Herr, T., *Bugs in the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications* (2016) New America, https://www.newamerica.org/oti/policy-papers/bugs-system/. *See* ISO/IEC 30111:2013, *Information Technology – Security Techniques – Vulnerability Handling*, International Standards Organization, (Nov. 1, 2013), http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231; ISO/IEC 29147:2014, *Information Technology – Security Techniques – Vulnerability Disclosure*, International Standards Organization, (Feb. 15, 2014), http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170.

preventing public disclosure becomes a more attractive option. This option does come with a downside; media coverage has not been favorable towards companies' attempts to silence researchers and, in many cases, the information is disclosed anyway.[21] Even when researchers notify the company of a flaw without public disclosure, the company may perceive notification as an implied threat or an attempt to extort. In some cases, companies are not prepared to receive and efficiently process a notification through an established disclosure process. For these and other reasons, companies may respond poorly, or not at all, to a researcher's attempt to share information about a flaw or vulnerability.

For researchers, publicly disclosing research results creates different kinds of risk. Depending on the circumstances and the method of disclosure, a researcher may face risks of harm to their reputation, employment, or legal standing. Examples of all three have been documented in the media.[22] In fact, disclosure is a common thread uniting nearly every documented example of security researchers experiencing unfavorable treatments as a result of their work. Although the majority of these incidents did not escalate beyond verbal or written threats of legal action, the FBI arrested and charged one researcher and investigated another.[23] In some cases, researchers withheld public disclosure in response to threats or other forms of pressure from companies that would be affected by the disclosure.[24]

Of the researchers we interviewed, few reported receiving threats related to a disclosure, either veiled or explicit. The researcher reporting the greatest number of threats often serves as a disclosure intermediary for other researchers. This subject reported that many of the researchers for whom the subject had performed a notification or disclosure did not want to notify the company themselves because of the risk they associated with notification. Other interview subjects reported being pressured by companies to keep quiet or to sign non-disclosure agreements (NDAs).

In addition to the subjects with negative first-hand experience related to disclosure, many more reported some level of concern or behavior modification related to disclosure practices. For one subject, the risk associated with notifying a company of a flaw or vulnerability varied

[21] *See* e.g., Tim Cushing, *Another Company Thinks The Best Way To Handle A Security Hole Is To Send A Lawyer After The Person Who Discovered It*, (May 7, 2015) *TechDirt*, https://www.techdirt.com/articles/20150506/11491630903/another-company-thinks-best-way-to-handle-security-hole-is-to-send-lawyer-after-person-who-discovered-it.shtml.

[22] *See, e.g.*, http://attrition.org/errata/legal_threats/.

[23] Robert Lemos, *Russian crypto expert arrested at Def Con*, (Mar. 2, 2002) CNET, https://www.cnet.com/news/russian-crypto-expert-arrested-at-def-con/; Kim Zetter, *Whistle-Blower Faces FBI Probe*, (Jul. 29, 2005) Wired, https://www.wired.com/2005/07/whistle-blower-faces-fbi-probe/.

[24] Darren Paulli, *Talk revealing p0wnable surveillance cams pulled after legal threats*, (Oct. 8, 2015) The Register, http://www.theregister.co.uk/2015/10/08/hitb_remote_exploit_ip_cameras/?mt=1444351029389.

according to the company's level of "sophistication," where more sophisticated entities posed a lower level of risk because of their willingness and ability to constructively engage with the researcher.[25]

For some, concerns about disclosure stemmed from the potential negative consequences for themselves or the company to which they might report a flaw. More specifically, some subjects avoided disclosures that would potentially create reputational harms for software or device companies because those harms could damage their own working relationships. One subject viewed such disclosures as harmful to the public perception of both the company and the researcher. Two researchers noted that professional relationships between companies and researchers, and the contractual obligations they entail (like non-disclosure and non-compete agreements) can have a chilling effect on a researcher's choice of projects. Others were concerned that disclosure might put end users or the general public at risk. On the flip-side of this concern, one subject noted the reputational benefits, both for the individual researcher and for the community at large, of careful disclosure practices.

3.4 Norms

Whether out of a desire to minimize legal risk, to mitigate risks to third parties, or to avoid reputational harms to themselves or the larger community, the researchers we interviewed expressed a variety of self-imposed norms regarding their research and disclosure practices. We observe that many of these norms coincide with certain elements of the CFAA in that they reflect a desire to avoid 1) crossing the line between authorized and unauthorized access to network-connected computers, 2) obtaining information from such computers, and 3) causing any kind of harm to another computer. Other practices were shaped by concerns about accessing, obtaining, or exposing potentially private information. Some researchers took certain actions or avoided certain practices to align with their perceptions of community standards. In some cases this self-regulation appeared to be driven by concerns about their own individual reputations, but in other cases the motivation seemed to derive from a desire to avoid damaging the public perception of the security research community.

3.4.1 Scanning practices

Several researchers reported a suite of practices in projects involving network scanning. First, subjects observed or otherwise indicated that although network scans were once considered

[25] Other researchers noted their perception of a lower degree of risk when the company offered a bug bounty program or had an accessible vulnerability reporting policy. One subject noted a preference for a vuln disclosure policy (over a bounty) because of the limits associated with bounty disclosures.

legally risky because of the potential for “exceeding authorized access” and “obtaining information” per the CFAA, they have become common practice. Within the confines of some of the norms discussed below, network scanning is no longer seen as a significant source of legal risk. However, several subjects who reported performing regular network scans also reported receiving threats and other expressions of disapproval from network operators and system administrators. Most subjects expressed a low-level of concern for this kind of feedback. In both academic and independent settings, researchers have modified their scanning practices in response to negative feedback; they began adding identifying and explanatory information to their scanning infrastructure to help operators understand the purpose of the scanning exercise and to facilitate their ability to opt-out of future scans.

3.4.2 Terms of Service / Logins

Perhaps in response to the CFAA bar against “exceeding authorization,” several subjects noted their avoidance (where possible) of scanning entities with TOS prohibiting scans. Others noted the difficulty of manually reading TOS on the scale necessary for massive scanning projects and the difficulty of accessing TOS from an Internet Protocol (IP) scan interface (i.e., one IP address may host many individual websites; whose TOS governs?). Perhaps following a similar motivation, several subjects avoided access to systems requiring login credentials. Many stated that they would not consider using “found” credentials to access a system. For some, even using default credentials was too risky. For others, using found credentials was acceptable for the purpose of testing their validity as long as the connection was terminated immediately after a successful login. In one subject’s opinion, this avoided the potentially risky “accessing” element of the CFAA. Other subjects noted that although they would not use found or stolen credentials, they saw no problems with creating their own accounts on public-facing systems for the purposes of accessing those accounts in their projects.

3.4.3 Data collection

For others, especially with regard to scanning projects, one way to reduce risk was to minimize or eliminate the collection of data from other computers. Almost half of our subjects reported privacy-related concerns regarding data collection. Subjects found a variety of methods by which they could perform scans for particular kinds of information without retrieving data from other computers. One researcher noted that file size played a part in their risk calculations, positing that some data packets are too small to contain sensitive information and therefore present a lower level of risk than larger packets. In some cases, data collection was either necessary for the project or desirable for other reasons. Subjects noted that, where data collection was unavoidable, they took precautions to minimize or avoid collecting personally identifying information (PII). This seemed driven in part by concerns about privacy-related legal issues and partly to avoid or minimize problems with institutional review boards (IRBs). Two researchers noted the practical problems and obligations arising from finding or obtaining files containing images depicting exploitation of minors.[26]

3.4.4 Exploiting vulnerabilities

There was some variation in how researchers approached the practice of exploiting a vulnerability as part of a project. This variation may be due to several factors, including the context in which the researcher considered exploiting the vulnerability, the purpose of executing the exploit, the kinds of research work normally performed by the subject, and the subjects' individual codes of ethics. One researcher reported avoiding the exploitation of any vulnerabilities for scanning projects, and also advised that vulnerability research has a higher level of legal risk than other kinds of research. Another observed that exploiting a vulnerability to gain access to or execute code on someone else's computer was unacceptable. One researcher reported avoiding the exploitation of vulnerabilities where there was a risk of harm to the vulnerable system or others.

3.4.5 Live systems

Avoiding risks to third parties was a common theme regarding testing of "live" systems. Three subjects reported avoiding work on live systems. Others reported a preference against testing live systems without consent of the owner(s). Some expressed a rule against "hacking" other people's systems or machines. It is unclear from the interviews, however, whether all subjects would define "live" systems in the same way.[27]

[26] While researchers may encounter such content in the course of their work, it was unclear if they understand the legal obligation to report such content to the National Center for Missing and Exploited Children (NCMEC).

[27] "Live" testing refers to testing systems that are in operational use. In a current proceeding before the Copyright Office and the Library of Congress, researchers are attempting to distinguish "live" testing from "real-world" settings – attempting to test systems in as close to a "live" setting as possible while minimizing risks of harm, damage, etc. – for security research because testing in "real world" settings creates more realistic vulnerability models than can be simulated in a lab and, for some systems, may be the only way to effectively test their security. *See* Reply Comments of Prof. Ed Felten, Prof. Alex Halderman, and Center for Democracy & Technology, Class 10 Computer Programs - Security Research, Library of Congress, Copyright Office, Exemptions to Permit Circumvention of Access Controls on Copyrighted Works, (March 14, 2018) https://www.copyright.gov/1201/2018/comments-031418/class10/Class_10_Reply_Felten_Halderman_CDT.pdf.

3.5 Misperceptions

All qualitative methods result in findings that were not expected when the research was designed. In this case, we encountered a few sets of what we will characterize as "misperceptions" about barriers to security research.

There were unexpected sources of chilling effects. For example, one subject described how a different part of the DMCA – the Section 512 provisions for the online removal of allegedly infringing material – chilled their research and their ability to speak about their research. In this scenario, a researcher would upload video in which they described or analyzed a particular security vulnerability to a hosting provider, only to have the video taken down in response to a notice of infringement. Section 512 requires providers, upon receiving notification of the presence of allegedly infringing material on their servers, to remove or block access to that material. Although user-generated video can potentially infringe another party's copyright, Section 512's "take down" provisions have been used improperly to protect non-copyright interests, such as by silencing speech that could harm business interests.

We also saw evidence that some researchers have a misperception that the statutory exemptions in DMCA Section 1201 may excuse certain activities when they do not. Notably, the statute does not exempt acts of circumvention performed out of "curiosity" or by scientists in their role as scientific investigators.

Finally, we saw evidence that repairing flaws and defending against the exploitation of vulnerabilities isn't always the main motivation for these researchers. Some rationalized that keeping particular vulnerabilities to themselves helps them catch bad actors online. In a few cases, researchers had serious concerns about potential risks that their work might pose to society at large, categories of people, or even specific individuals; these considerations tended to stop a given project. Also, researchers were less inclined to release the tools from a particular project or hack if it would really only result in net harm – e.g., information solely useful for copyright infringement or denial-of-service attacks.

4 Building a 'Risk Basis'

This research project initially set out to better define what a code of conduct for security research might look like. As the project progressed, it became clear that no unified code of conduct could easily apply to all the various activities undertaken by security researchers, hackers, and those that work in information, computer, and network security. Moreover, these boundaries are constantly in flux, changing in response to the developing, accepted, and rejected practices of academics, white hats, and black hats alike.

Instead of a code of conduct, we decided to construct a “risk basis.” For each genre of activity in which a security researcher or hacker may engage, we identify lower- and higher-risk methods of performing that activity. The intent is to provide some guidance as to activities that are lower-risk or that may need more careful design to mitigate risk. Although we mention other risks, such as reputational harm, we are primarily concerned with risk of liability under United States law. Many of these perceived risks derive from a few activities necessary for violation of these laws. Accessing or exceeding authorized access to a protected computer, obtaining information from it, or circumventing access controls protecting copyrighted works are some of the more influential sources of risk, yet a single research project could require all three.

Here, we articulate a set of security research activities and, based on the precedent or perception of our interview subjects, the relative levels of risk associated with various methods of performing those activities.[28]

4.1 Accessing computers

Other than the methods of testing for vulnerabilities via network scanning (e.g., Shellshock described later), researchers viewed gaining access to computers they do not own as a high-risk activity. ***Avoiding accessing any computers to which the researcher does not have lawful and legitimate access minimizes risk.***

However, the trend toward software-as-a-service in many IoT and cloud computing contexts means that more security research projects now involve networks and thus become entangled with the CFAA’s notion of a “protected computer.”[29] This will generally increase the legal risk for research performed on components that are now only reachable across a network boundary.

4.1.1 Accessing using credentials

Security researchers occasionally find login credentials in the course of their work. For instance, credentials may be found through the analysis of malware or observation of malicious hacker forums, or public services such as Twitter or Pastebin. ***Researchers view using those credentials to gain access to their related accounts as very risky.*** Where the benefit of using found credentials is sufficiently high, researchers may minimize their risk by severing the connection

[28] For a summary of this risk basis, see Appendix B.
[29] *See* note 16, *supra*.

immediately after a successful login, but before receiving any additional data. This minimizes risk under both the "obtaining" and "accessing" prongs of the CFAA. Additionally, researchers can minimize risk by creating their own accounts on the target system, for example, by signing up for an account, and then accessing that account instead of accessing someone else's account and information.

Researchers perceived the risk for using credentials in some contexts as relatively low, but still unacceptable. For example, some samples of malware contain embedded credentials that security researchers could use to login to or otherwise access the systems controlling or distributing the malware. This access could help study malicious attackers' infrastructure, find lists of infected targets, and gain other information to curb the spread of malicious software. However, using those credentials would involve accessing a target computer and obtaining information from it, likely violating the CFAA. In these cases, ***it may be more appropriate and less risky for researchers to communicate the analysis and credentials directly to law enforcement rather than attempting to access the systems.***

4.1.2 Accessing computers through network scanning

For researchers performing network scanning, much of the risk they face stems from the CFAA. In particular, the statute's "obtaining" and "accessing" prongs seem to have shaped some scanning practices. In general, scanning methods that do not acquire or obtain data stored in other computers are perceived as less risky than methods that do. ***Accordingly, scanning methods that minimize the amount of data researchers obtain will tend to reduce the perceived legal risk associated with that aspect of the project.***

Because network scanning necessarily involves at least some interaction with other computers, and because the nature of those interactions may not enable server operators to effectively define the scope of "authorized access," the potential for reducing risk under the CFAA's "accessing" prong is less clear. Considering the absence of clearly defined limits and the impracticality of obtaining consent on a network scale prior to scanning, researchers instead take measures to improve the perceived legitimacy of their scan. For instance, including information (e.g., in packet headers) that explains the nature and purpose of the scan, identifying the researcher or entity performing the scan, and providing a mechanism by which operators can opt-out of future scans are methods to both demonstrate the benign intent of the researcher and prevent future interactions that might "exceed authorized access." ***Scanning methods that employ transparency and opt-out mechanisms are perceived to be less risky.***

Where operators have expressed some limits on authorized access, such as through Terms of Service, researchers can minimize their legal risk by strict adherence to the terms. Where terms of service explicitly address the kinds of access researchers anticipate their work will entail, whether through a vulnerability disclosure policy, a bug bounty program, or clear language prohibiting specific practices, risk assessment is more certain. However, where the scope of authorized access is unclear or does not address the type of interaction involved in a scan, researchers may be forced to assume some risk to continue scanning. The scale of many scanning projects makes analysis of and compliance with Terms of Service impractical, as the number of target systems are potentially in the hundreds of millions. ***As a result, scanning researchers may only be able to reduce their risk by selectively reading the TOS for entities they deem most likely to take legal action, by excluding entities known for their objection to scans, and/or by designing scanning infrastructure that can attempt to detect language prohibiting these activities*.**[30]

4.2 Obtaining information

4.2.1 Exploiting vulnerabilities to obtain data

Where scanning or other methods of security testing involve exploiting a vulnerability, researchers assume some risk based on a view that exploiting a vulnerability is necessarily an "unauthorized access" under the CFAA. However, researchers that exploit vulnerabilities may still be able to reduce their legal risk by eliminating or minimizing the amount of information they obtain that originates from other computers. The Heartbleed vulnerability allows attackers to "deposit" a small packet of data (e.g., "dog") on a vulnerable machine, and then later ask for that packet back while also obtaining additional data from the vulnerable machine's own memory (e.g., "dogPASSWORD"). However, in one method of testing for the Heartbleed vulnerability, researchers send a request for zero bytes. Receipt of an empty (zero-length) return value indicates the presence of the vulnerability without "obtaining" information from the vulnerable computer. In another method, researchers would "pack" the target system's memory with their own data, then ask the vulnerable computer to return only the "packed" data such that any data returned was the researcher's own data instead of potentially-sensitive data from the target system. ***Researchers perceive their legal risks to increase with the amount of data transmitted out of the vulnerable computer, especially for data that originated on the vulnerable machines.***

[30] The latter would require some form of human intervention to be precise.

Similarly, in testing for the Shellshock vulnerability, researchers necessarily exceed authorized access because the vulnerability grants access to a command-line environment (a shell).[31] In many cases these shells posses administrative (root) privileges and are able to execute administrative commands as well as read and write data on the target system. The only way to prove the presence of the vulnerability is to exercise this administrative privilege to execute commands. Types of minimally risky commands include executing a "sleep" command or causing the computer to send a minimal "ping" message back to the researcher that contains no privileged data. Using the "sleep" command, researchers send packets out to the network with instructions to tell computers to pause for a few seconds, then count vulnerable systems by checking the differences in delays of scanning packets to infer the presence of systems where the sleep command worked and are thus vulnerable.[32] This method doesn't result in the target system returning any data at all.

Another option does involve returning data: the researcher can instruct the vulnerable computer to send only a single packet – a "ping" or Internet Control Message Protocol (ICMP) message. The researcher's receipt of the ping proves the presence of the vulnerability because the target computer performed a command that would otherwise only be available to the computer's administrators. It is unclear whether this would satisfy the "obtaining" prong of the CFAA; ping packets do not contain any privileged information from the target computer, but they are constructed and transmitted by the target computer. ***Minimal data transfer, such as retrieving a packet of zero bytes or causing the transmission of a single ping packet, is perceived as lower risk because it reduces the potential for the researcher to obtain potentially sensitive data.***

4.2.2 Downloading data

In terms of downloading or otherwise "obtaining" data, researchers noted a few strategies for minimizing risk. As discussed above, both the Heartbleed and Shellshock vulnerabilities[33] had the potential to allow researchers to access a considerable amount of data – 64 kilobytes (KB) in the case of Heartbleed and a potentially arbitrary amount of data in the case of Shellshock. However, if a researcher tests Heartbleed and receives a single byte back instead of 64,000 bytes, or receives a single ping in testing for Shellshock, the researcher is unlikely to obtain sensitive data or cause harm to the target system, potentially reducing risk. ***Inferring a property or characteristic about a target system without obtaining or transmitting data would most***

[31] John Graham-Cumming, *Inside Shellshock: How hackers are using it to exploit systems* (September 30, 2014), Cloudflare Blog, https://blog.cloudflare.com/inside-shellshock/.
[32] *See shellshock-scanner*, https://github.com/gry/shellshock-scanner.
[33] *See* 4.2.1 Exploiting vulnerabilities to obtain information, supra.

effectively minimize risk. Where obtaining some data is unavoidable, researchers may reduce their risk if they obtain only a negligible amount.

There has been an unfortunate uptick in instances of abandoned or unsecured data on cloud services such as Amazon EC2 and Microsoft Azure, where data owners have not properly decommissioned databases with hundreds of millions of records involving personal and proprietary data.[34] Although obtaining data may be squarely covered by the CFAA, security researchers who investigate cloud data breaches often need to download the data for several reasons. First, looking at data can help a security researcher determine its original source and thereby help identify and contact the data owner (or their cloud service provider) who can then begin to secure vulnerable resources in a timely manner. Second, through data analysis, researchers may be better able to determine the sensitivity of the data and respond accordingly. In some cases, the scope and sensitivity of the exposed data and services may warrant disclosure beyond the data owner, such as to authorities like the FBI. For example, sensitive medical records with protected health information (PHI) may need to be secured quickly, with notification to the Department of Health and Human Services' Office of Civil Rights and potentially the FBI. ***In cases where downloading data is an important part of vulnerability handling, to minimize risk, researchers should practice data minimization techniques, making an effort to download only enough for the relevant analysis, and securely disposing of it afterwards.***

[34] *See, e.g.*, Dan Goodin, *Thousands of servers found leaking 750MB worth of passwords and keys*, (Mar. 22, 2018) Ars Technica, https://arstechnica.com/information-technology/2018/03/thousands-of-servers-found-leaking-750-mb-worth-of-passwords-and-keys/; John Leyden, *Sensitive client emails, usernames, passwords exposed in Deloitte hack*, (Sep. 25, 2017) The Register, https://www.theregister.co.uk/2017/09/25/deloitte_email_breach/; Zack Whittaker, *Accenture left a huge trove of highly sensitive data on exposed servers,* (Oct. 10, 2017) ZDNet, http://www.zdnet.com/article/accenture-left-a-huge-trove-of-client-passwords-on-exposed-servers/; Dell Cameron and Kate Conger, *GOP Data Firm Accidentally Leaks Personal Details of Nearly 200 Million American Voters*, (Jun. 19, 2017) Gizmodo, https://gizmodo.com/gop-data-firm-accidentally-leaks-personal-details-of-ne-1796211612; Dan Goodin, *Pentagon Contractor leaves social media spy archive wide open on Amazon*, (Nov. 18, 2017) Ars Technica, https://arstechnica.com/information-technology/2017/11/vast-archive-from-pentagon-intel-gathering-operation-left-open-on-amazon/; Elizabeth Weise, *Info on 1.8 million Chicago voters exposed on Amazon server*, (Aug. 18, 2017) USA Today, https://www.usatoday.com/story/tech/2017/08/18/information-1-8-million-chicago-voters-exposed/579656001/; Asha McLean, *Alteryx S3 leak leaves 123m American households exposed*, (Dec. 19, 2017) ZDNet, http://www.zdnet.com/article/alteryx-s3-leak-leaves-120m-american-households-exposed/

4.3 Circumventing access controls

In terms of circumventing access controls or technical protection measures (TPMs), researchers perceived less risk for these activities in controlled, non-networked situations because they could retain control over the effects and the knowledge of their work.

In addition, ***researchers recognize that entertainment and media systems may both be more likely to be networked and are functions most closely aligned with the DMCA's core goal of limiting copyright infringement.*** Many new forms of entertainment and media systems use two-way communication networks to keep content fresh, adapt content to network conditions, and fulfill other functions. Since CFAA liability has been interpreted to apply to activities involving any computer communicating over a network across state lines, accessing these systems beyond the limits set by their terms of use or licensing agreements likely implicates the CFAA. Additionally, because many forms of entertainment and media systems use DRM technologies, circumventing those controls in the course of research will undoubtedly implicate the DMCA. Although security researchers might otherwise be eligible for either the statutory exemption or the current temporary exemption for security testing, both contain clauses requiring compliance with all applicable laws, including the CFAA. Therefore, ***to work on network-connected devices or systems protected by access controls, researchers may risk liability under both the CFAA and the DMCA, potentially compounding risk*****.** However, perhaps due to the accommodations in the statute or the relevant case law, researchers had the impression that circumvention accomplished for interoperability purposes was less risky and less likely to attract legal threats.[35]

4.4 Disclosing vulnerabilities

Disclosing a vulnerability – whether privately to the relevant company, directly to the public, or through a coordinated effort – can be a legally risky act. Many legal threats against researchers involve disclosure in some manner; in most cases, disclosure or a statement of intent to disclose triggers the legal response. ***However, coordinated disclosure with adequate communication among knowledgeable parties and attention to fixing a flaw minimizes risk of legal repercussions.*** Researchers use a variety of signals to manage risk of legal threats related to disclosure, including a firm's previous treatment of researchers, presence of a vulnerability disclosure policy, and to a lesser extent, a bug bounty program. Naturally, it may be more risky to attempt vulnerability disclosure with a firm that has threatened researchers or has poorly

[35] The statute contains a permanent exemption for reverse engineering to achieve interoperability with other computer programs. 17 U.S.C. § 1201(f). See also, n. 8,9, *supra*, discussing the different approaches courts have taken depending on the kind of copyrighted works involved.

handled vulnerability disclosure previously. ***The presence of a vulnerability disclosure policy appears to reduce the perceived risk of disclosure; it serves as important signal that the firm on the receiving end of a vulnerability notification is more likely to have staff that understand security concepts and are willing to engage in coordination to secure their products and repair flaws.***

To reduce their personal risks related to vulnerability disclosure, security researchers may choose to remain anonymous and instead use intermediaries to handle disclosures. Complex forces can shape disclosure. For example, a security researcher in one firm may find a vulnerability in a client's or partner firm's product, but elements of those business relationships may create sufficient friction or reputational risk to prevent disclosure. In these cases, a researcher may choose to disclose the vulnerability using an intermediary to avoid personal involvement and the potential negative consequences resulting from the disclosure. These intermediaries can take a number of different forms, from Computer Emergency Response Teams (CERTs), to other researchers who are unencumbered by the same contractual or reputational restrictions, to journalists who may be interested in covering the details of a vulnerability. Independent or non-academic researchers – who are more likely to get a cold shoulder from businesses than academic researchers[36] – may improve their disclosure outcomes by choosing an intermediary that has a more substantial reputation for past good work or the gravitas of academic status.

4.5 Testing live systems

When considering security research involving "live" systems, currently operating systems outside of an isolated controlled lab, ***researchers tended to see less risk in projects involving more isolated systems*.** However, the internet and World Wide Web are necessarily live systems, which also support many instances of remote computing interactions at all times. Therefore, some types of security research involving the internet and web are fundamentally about testing live systems and real data; these research questions cannot be answered in a lab.

Outside of network interaction on the internet and World Wide Web, researchers perceive considerable risk in testing certain kinds of live systems, especially cyber-physical systems. For researchers, testing these "smart" systems that include engineered interacting networks of

[36] Alexander Gamero-Garrido, Stefan Savage, Kirill Levchenko, and Alex C. Snoeren. "Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research," In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*. ACM, New York, NY, USA, 1501-1513. DOI: https://doi.org/10.1145/3133956.3134047.

physical and computational components"[37] is risky because of the potential for real-world physical harm. Likewise researchers cannot easily get samples of certain kinds of systems that they would like to test, from voting systems to airplanes to industrial control systems. Researchers viewed mounting experiments on live examples of these systems as categorically unethical and very risky. ***In general, interactions with live systems that could potentially cause harm in the physical world or invasions of privacy are perceived as too risky to pursue, unless the system can be replicated and studied in a lab environment, and effects on real people minimized.***

5 Conclusion

As we have shown, the complex forces that may limit or encourage cybersecurity research and information security analyses are not intractable. Taking the pulse of the community about the factors shaping their work can provide useful guidance on how hackers and security researchers may limit their risks of threats and liability under the law. Future work in this vein includes socializing, validating, and getting feedback on this risk basis to understand its practical utility and to correct any oversights or mistakes incorporated due to the modest size of our investigation. While it may be impossible or unwise to develop a "hacker code of conduct," security researchers, information security professionals, independent researchers, and hackers will be increasingly pressured to present clear distinctions between patently good and bad faith projects.

**Appendix A: Qualitative Interview Instrument || ** *(please see attached)*

Appendix B: Summary of a Risk Basis for Security Research || *(please see attached)*

[37] NIST Cyber-Physical Systems Working Group, "A Framework for Cyber-Physical Systems", (May 2016), available at: https://pages.nist.gov/cpspwg/ .

CENTER FOR
DEMOCRACY
& TECHNOLOGY

Interview Protocol

Assessing chilling effects to security researchers semi-structured qualitative interview protocol. (protocol v3, 8 July 2016.)

Read: We'll start the interview with some simple demographic questions and questions about your background and experience as a [security researcher/hacker/etc]. We'll then ask you questions about considerations you take into account in a new project and specific kinds of chilling effects you have faced or are aware of along a number of subjects (DMCA, CFAA, IRBs/peer review, and norms). Finally, we'll ask you some general questions about being a security researcher. Do you have any questions before we get started?

(1) Demographic Questions:

1. What ethnic background do you identify with?
2. What is your approximate age? 20-25, 26-30, etc.?
   2.1. Under 18, 18-24, 25-44, 45-64, 65+
3. (Note participant's perceived gender, write down in notes.)

(2) Background:

1. How long have you been engaged in security research?
   1.1. Can you describe for us the security related work or research you do?
   1.2. Alternatively, if you don't actively do security research, how do vulnerabilities and fixing them factor into your work now and in the past?
2. Is security research part of your employment? a hobby?
3. Describe the path that brought to the work you do now? Why did you decide to become a security researcher?

(3) Chilling Effects (1):

1. General:
   1.1. What are the considerations you take into account when deciding to hack on a new project, device, or piece of software?
   1.2. How often do you consult a lawyer before, during, or after a project?

1.2.1. Do you have a "go to" lawyer or organization for advice about how the law impacts your work?

1.2.2. (If necessary:) have you spoken to a lawyer before you started a project? while engaged in a project? or after a project was complete?

1.3. To what extent has your work put you in personal legal jeapordy? (This can be as small as a lawyer letter or as big as a lawsuit or prosecution.)

1.3.1. Have you been verbally threatened by a manufacturer or "target" of your research?

1.3.2. Have you received a Cease & Desist letter stemming from your work? (Can we see a copy to better understand how legal threats are structured and delivered?)

1.4. What kind of reputational effects exist here?

1.4.1. Do you suffer from not being able to publish things or work in certain areas due to legal risks?

1.4.2. Similarly, are there circumstances in which controversy surrounding publication may improve your reputation?

1.4.3. Do you do anything to neutralize potential reputational risks or to encourage publication controversy?

1.5. Do you design specific investigations or hacking projects in a way that minimizes risks to you?

1.5.1. Do you take into account ethical considerations when thinking about new projects?

2. DMCA

2.1. To what extent does your work involve circumvention? (Not censorship circumvention or network circumvention, but circumventing access controls, technical protection measures, or other usually cryptographic locks on software, devices, and systems.)

2.1.1. What kinds of safeguards do you put into place when engaging in circumvention research?

3. CFAA

3.1. To what extent does your work involve testing internet or web services?

3.2. Do you read Terms of Service?

3.2.1. If so, what do you look for? If not, why not?

3.3. Have you created tools that scan internet endpoints for open ports?

3.4. Have you created tools that do more complex kinds of endpoint evaluation? (**Only if they're confused:** for example, scanning code that might check to see if a server is vulnerable to a particular exploit?)

3.4.1. How far do you think you should be able to go here?

3.4.2. For example, if you exploit a vulnerability to evaluate whether or not a server is vulnerable, is that too far?

3.4.3. What about "testing" what purport to be stolen authentication credentials by trying to authenticate?

4. IRBs, conference committees, journal boards

4.1. Have you ever had push back or other difficulties in publishing your work in a venue of your choice, be it a journal or conference?

4.1.1. Have you had a conference refuse a talk or paper?

4.1.2. Have you had a venue "pull" a talk/paper after acceptance?

4.1.3. Have you had any disclaimer placed on your work by a program committee or publication?

4.1.4. Have you ever had a dispute with a client or employer about publishing your work?

4.2. Do you work with an IRB to clear research that you work on for risks to human subjects?

4.2.1. If not: Do you understand why the academic community appeals to IRB structures to vet their research?

4.2.1.1. Do you think something like this would be useful for the security research/hacker community?

4.2.1.2. (Potentially, describe the new Tor Research Safety Board: https://research.torproject.org/safetyboard.html)

4.2.2. If so: What is your experience with your IRB like?

4.2.2.1. Do you think they're overly strict? Too lax?

4.2.2.2. Have you developed methods to address risks to humans from interacting with an IRB?

5. Norms

5.1. How far is "too far" when testing?

5.1.1. Can a tester use credentials to gain access to see if they work?

5.1.2. What about testing live systems?

5.2. Are there forms of research you’ve considered but don’t do because that work “is just not done” in your field?

6. Bug bounties and Vuln Disclosure Programs

6.1. What role do bug bounty programs play in chilling effects to your work?

6.1.1. Are you more likely to hack on a thing because they have a bug bounty?

6.1.2. Do the terms of bug bounty programs provide adequate “rules of engagement” for you or are they often too limiting (or both)?

6.2. To what extent do vulnerability disclosure policies shape how you do your work or how you disclose findings?

Follow-on General Questions:

1. To what extent do chilling effects like those we’ve been discussing change research focuses?

1.1. Are there examples of research you cannot do due to fears of legal consequences?

1.2. Do you change research efforts and research designs to be less likely to suffer legal consequences?

1.2.1. Do you work with regulators, the press, or other colleagues (in terms of validation of findings) to reduce the likelihood of retaliation or legal threats?

2. How do these chilling effects affect others in your line of work?

2.1. Do you know of any examples where legal mechanisms were brought to bear on a security researcher that stood out to you?

3. Are there other sources of chilling effects on your work that we did not talk about?

4. Are there resources (tools, guides, services) that you think could make it easier to do your work free from chills or negative influences?

5. Do you know of anyone else that would be good for us to talk to about this subject?

CENTER FOR
DEMOCRACY
& TECHNOLOGY

Summary of a Risk Basis for Security Research

The legal, ethical, and practical boundaries for security research are constantly in flux, changing in response to the development, acceptance, or rejection of practices of academics, white hats, and black hats alike. Because this dynamic environment makes it difficult to establish a unified code of conduct, we decided instead to construct a "risk basis" to provide some guidance as to activities that are lower-risk or that may need more careful design to mitigate risk.

This basis focuses primarily on risk of liability under United States law and derives largely from a few activities necessary for violation of these laws. The following are guidelines we observed for mitigating the legal risks associated with performing security research.

Accessing "protected" computers

- Avoiding accessing any computers to which the researcher does not have lawful and legitimate access minimizes risk.
- Researchers view using found credentials to gain access to accounts as very risky.
- Where credentials are found, it may be more appropriate and less risky for researchers to communicate the analysis and credentials directly to law enforcement rather than attempting to access the systems.
- Scanning methods that minimize the amount of data researchers obtain will tend to reduce the perceived legal risk associated with that aspect of the project.
- Scanning methods that employ transparency and opt-out mechanisms are perceived to be less risky.
- Scanning researchers may be able to reduce their risk by selectively reading the TOS for entities they deem most likely to take legal action, by excluding entities known for their objection to scans, and/or by designing scanning infrastructure that can attempt to detect language prohibiting these activities.

Obtaining information from "protected" computers

- Where scanning or other methods of security testing involve exploiting a vulnerability, researchers assume some risk based on a view that exploiting a vulnerability is necessarily an "unauthorized access" under the CFAA.
- Researchers perceive their legal risks to increase with the amount of data transmitted out of the vulnerable computer, especially for data that originated on the vulnerable machines.
- Minimal data transfer, such as retrieving a packet of zero bytes or causing the transmission of a single ping packet, is perceived as lower risk because it reduces the potential for the researcher to obtain potentially sensitive data.

- Inferring a property or characteristic about a target system without obtaining or transmitting data would most effectively minimize risk. Where obtaining some data is unavoidable, researchers may reduce their risk if they obtain only a negligible amount.
- In cases where downloading data is an important part of vulnerability handling, to minimize risk, researchers should practice data minimization techniques, making an effort to download only enough for the relevant analysis, and securely disposing of it afterwards.

Circumventing access controls

- In terms of circumventing access controls or technical protection measures (TPMs), researchers perceived less risk for these activities in controlled, non-networked situations because they could retain control over the effects and the knowledge of their work.
- Researchers recognize that entertainment and media systems may both be more likely to be networked and are functions most closely aligned with the DMCA's core goal of limiting copyright infringement.
- Work on network-connected devices or systems protected by access controls may risk liability under both the CFAA and the DMCA, potentially compounding risk.

Disclosing vulnerabilities

- Coordinated disclosure with adequate communication among knowledgeable parties and attention to fixing a flaw minimizes risk of legal repercussions.
- The presence of a vulnerability disclosure policy appears to reduce the perceived risk of disclosure; it serves as important signal that the firm on the receiving end of a vulnerability notification is more likely to have staff that understand security concepts and are willing to engage in coordination to secure their products and repair flaws.
- To reduce their personal risks related to vulnerability disclosure, security researchers may choose to remain anonymous and instead use intermediaries to handle disclosures.

Testing

- Researchers tended to see less risk in projects involving more isolated systems.
- In general, interactions with live systems that could potentially cause harm in the physical world or invasions of privacy are perceived as too risky to pursue, unless the system can be replicated and studied in a lab environment, and effects on real people minimized.