A Researcher's Guide to Some Legal Risks of Security Research

Sunoo Park
Harvard Law School

Kendra Albert
Harvard Law School

October 2020

Contents

1 About this Guide **2**

2 What do we mean by legal risk? **3**
2.1 Types of legal liability 4
2.2 Cease and desist letters 5

3 What kinds of security research raise legal risk? **6**
3.1 CFAA (Computer Fraud and Abuse Act) 8
3.2 Copyright law 10
3.3 DMCA §1201 (Digital Millennium Copyright Act on circumvention) 13
3.4 Contract law 18
3.5 Trade secret law 22
3.6 ECPA (Electronic Communications Privacy Act) 22
3.7 Export controls 23

4 FAQ on getting and working with an attorney **27**

5 Conclusion **30**

6 About the authors **31**

A collaboration of the

CYBERLAW CLINIC
HARVARD LAW SCHOOL | BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY

and the

ELECTRONIC FRONTIER FOUNDATION

---

1 About this Guide

Who is it for? This guide is intended for non-lawyers interested in getting a general idea of when U.S. law can create legal risk for security researchers.

What does it cover? *This guide overviews broad areas of potential legal risk related to security research, and the types of security research likely implicated.* We hope it will serve as a useful starting point for concerned researchers and others. While the guide covers what we see as the main areas of legal risk for security researchers, it is not exhaustive. It also doesn't create a lawyer-client relationship between you and the authors.

This guide focuses on U.S. law, and mostly federal law. Different U.S. states and jurisdictions may have different laws, and even different interpretations of the same federal law.[1] This guide does not do a state-by-state analysis, but rather focuses on federal law and how it is interpreted by most states. To determine which states' law applies to your specific situation, consult a lawyer.

This guide does *not* discuss risks associated with security research under non-U.S. legal systems. Your activity may raise legal risks in legal systems outside of the U.S. if it takes place or has impacts outside the U.S., or involves or impacts people who are governed by non-U.S. legal systems. Similarly, your activity may be subject to U.S. legal liability (as well as liability under your local law) even if it occurs primarily outside the U.S., if it has impacts in the U.S. or involves or involves U.S. people and/or equipment.[2]

Finally, if your research involves human subjects and is aiming to produce generalizable knowledge,[3] you should consult an institutional review board (IRB) or ethical review committee to ensure that you are in compliance with human testing rules, which are outside the scope of this Guide.

How is it organized? Section 2 covers preliminaries: what we mean by legal risk, how legal risk can lead to liability, and different types of legal liability (civil or criminal). Section 2.2 gives advice on how to approach cease and desist letters—one common way that security researchers experience legal threats.

Section 3 then gets into the law: we outline seven main areas of U.S. law that may create legal risk for security researchers, and break down the types of research activities implicated by each of these areas (see Table 1 for a one-page summary). The seven subsections of Section 3 discuss each area of law in more detail, and illustrates how the law would apply to some example scenarios.

Section 4 discusses some common questions about getting and working with an attorney in the context of security research. Finally, Section 5 concludes, and

[1] Although all U.S. courts must follow the U.S. Supreme Court's interpretation of federal law, they may have differing interpretations where the Supreme Court has not (yet) weighed in.

[2] Some relevant U.S. laws have broad, seemingly worldwide scope: notably, the Computer Fraud and Abuse Act (CFAA), which will be discussed in more detail in Section 3.1 below. While American laws aren't directly enforceable abroad, appearing to violate such broadly scoped American laws may still cause trouble for those who live outside the U.S.

[3] I.e., aiming to draw conclusions beyond the specific human subjects your research is examining—practically, this covers almost all academic or technical research.

Section 6 provides background on the authors, the Cyberlaw Clinic at Harvard Law School, and the EFF.

How can I get more advice? If you need help finding a lawyer qualified to advise on legal risks of specific security research (in the U.S. or elsewhere), there are a number of sources that offer referrals, including the Electronic Frontier Foundation (email info@eff.org). In certain circumstances, the Cyberlaw Clinic may also be able to help (you can fill out the Clinic's intake form[4]). If you are concerned about getting a(n affordable and sympathetic) lawyer, you may also find Section 4 ("FAQ on getting and working with an attorney") helpful.

2 What do we mean by legal risk?

By "legally risky," we mean activities that carry non-trivial risk of either civil or criminal liability (these two terms are explained below). When criminal liability may be involved, we specify it explicitly. When we say an activity is legally risky, we do not mean that it is certain to carry legal liability. This lack of certainty is both because liability will depend on the specific context, details, and location of the activity concerned, and because unfortunately, the legal status of security research activities is often ambiguous given the broad language of existing laws and the limited number of court cases in the U.S. to date. In a common law system like the U.S., the legality of various security research activities should slowly become more clear as more cases are decided by the courts, giving us a better idea of how the law will likely be interpreted in future similar cases.

Note that even if an activity carries legal liability *in principle*, whether that liability will be realized *in practice* depends on whether the U.S. government or other parties decide to take you to court for it, which will depend on the incentives and skills of the parties involved. That said, the legal attitude of institutions[5] often focuses on risk aversion over testing the waters (especially in areas of unsettled law), even when a research activity seems likely legal and/or realistically unlikely to provoke litigation—this can sometimes be a source of tension between institutional pressures and researchers' interests, especially when (as often) institutional lawyers are not well acquainted with security research and the specific legal and ethical issues it raises.

Security research is, of course, essential to designing, building, and maintaining secure systems. Making security research activities illegal, and casting doubt on their legality, undermines the security of the very systems that computer crime laws purport to protect.[6] It is alarming that the law does not more clearly distinguish between security research and computer crimes, and

[4] https://blogs.harvard.edu/cyberlawclinic/clients/potential-clients

[5] E.g., universities or other employers of researchers.

[6] *See* Brief for Computer Security Researchers et al. as of Amici Curiae in Supp. of Pet'r, *Van Buren v. United States*, No. 19-783 (U.S. filed July 8, 2020), https://www.eff.org/document/van-buren-eff-security-researchers-amicus-brief; Jack Cable et al., *Response to Voatz's Supreme Court Amicus Brief*, https://disclose.io/voatz-response-letter [https://perma.cc/8YXK-9WY2].

we believe this situation needs to change.[7] That said, this guide has the pragmatic focus of accurately describing the current legal landscape and helping researchers assess their risk; it largely omits commentary on the wisdom of the legal approaches described.

2.1 Types of legal liability

Legal liability may be civil or criminal.

Civil liability generally occurs in a lawsuit initiated by a private party, when the court orders the defendant (i.e., the person sued) to pay a certain amount of money and/or to comply with a certain order (e.g., to stop the activity that the lawsuit is complaining of). Not complying with such an order would risk further legal sanctions.

Often, the private parties who could initiate a lawsuit—software and hardware vendors, website owners, and others—will not go through the expense and inconvenience of bringing a lawsuit against security researchers. Among other considerations, aggressively bringing lawsuits against individuals may damage an organization's reputation. In rare cases, however, they could consider it worthwhile to sue despite expecting to lose money (or even to lose the case) in hopes of deterring future similar activity. In our experience, organizations with more mature security programs are less likely to threaten litigation because they understand that such threats reduce the chances of later reports of security flaws. However, larger organizations without particular expertise in computer security may be more inclined to respond to a vulnerability report with cease and desist letters or legal threats. Sometimes, the prominence of a security researcher might influence a decision to file suit, and this might cut either way: suing a prominent researcher might be seen as a high-profile deterrent strategy, but on the other hand, prominent researchers' reputation and resources might mean more risk of publicity backlash against the organization suing.

Criminal liability occurs in cases that are initiated by the government accusing the defendant of a crime. Such liability may involve paying a fine and/or incarceration. A defendant found liable in a criminal case will also have a criminal record. Civil liability, by contrast, does not create a criminal record and cannot result in incarceration. The government has broad discretion over whether to criminally prosecute an individual, even when it knows or suspects a crime has technically been committed. State governments, the federal government, and tribal governments can prosecute crimes.

[7] It would be better if the law would carve out specific exemptions for security research and make ample provision for individuals to demonstrate lack of criminal intent. We have seen some steps in a positive direction, including notably, the recent DMCA §1201 exemption, which resulted from important efforts by researchers, activists, and others. We discuss the DMCA later in this guide. If you're a researcher, consider how you and your colleagues' voices could help push the law in the right direction!

Civil liability applies to a larger class of conduct than criminal liability, and you may be found civilly liable for conduct that is not a crime. (For example, civil wrongs that are not crimes include breaching a contract or harming someone through not being careful enough.)

2.2 Cease and desist letters

Before we dive into the law, it may be useful to talk about one common way that security researchers experience civil legal threats: through *cease and desist (C&D) letters*.

Although C&D letters can appear intimidating, getting one does not mean that you are being sued, or that you will be sued. It also doesn't necessarily mean anything about the sender's chances of winning if they did decide to sue, or that you will be liable if you disobey the letter. In other words, there's no magical legal significance to a C&D letter: a C&D letter is not required in order to sue, and does not necessarily mean that someone has adequate grounds to sue. C&D letters often lay out the main legal theory that the person threatening to sue would use if they did sue, but it's also worth noting that sometimes C&D letters can play fast and loose with the law—especially if they're not signed by a specific lawyer, and sometimes even if they are.

Here are some questions that can be helpful to ask when you receive a cease and desist letter.

Who sent it? Is it signed by "legal team," a specific in-house lawyer, or an external law firm? If an external law firm, do they specialize in general business law or do they primarily do litigation?

Generally speaking, a letter from an in-house legal team (especially if it is not signed by a specific lawyer) is more likely to be boilerplate and less likely to represent a specific legal threat than an external law firm that specializes in litigation. That doesn't mean you should necessarily ignore an unsigned letter, but it's reasonable to regard it with more skepticism.

How much information does it have about your research? How much knowledge does it demonstrate about the area?

If a C&D is your first interaction with a person or company, it can be a valuable opportunity to learn more about the level of sophistication of the organization you are dealing with. If the letter misunderstands your work or demonstrates a lack of security knowledge, it may create space to have a conversation about how the organization could better respond to security researchers. (On the other hand, some organizations aren't acting in good faith, and so can be difficult or inadvisable to engage with. Use your judgment and consult with others as helpful.)

What law does it cite and how much detail does it go into?

Although the absence of legal citations doesn't mean that there aren't legal claims to be brought, a lack of specificity can be a sign that the

organization is less interested or able to pursue legal action, or that they're bluffing.

At the same time, just because a letter does include citations to specific laws or court cases, that doesn't necessarily mean the sender is right or even that those sources say what the sender claims. A qualified attorney can help evaluate this.

Does it ask for a response by a particular date?

C&Ds are not issued by courts, and senders are usually willing to negotiate the response date, especially if you're in the process of attempting to find an attorney. It is not unreasonable to ask for more time (politely).

You are neither required to respond to a cease and desist letter nor, in general, to comply with the requests in it. (In certain circumstances, a C&D letter may affect your CFAA liability, as discussed in Section 3.1. If a C&D discusses "authorization" or "permission" and/or refers to the CFAA, it is especially advisable to find legal counsel.)

While a C&D letter may not create any legal obligations, it can be a good idea to find legal counsel if you're confronted with one: to assess the level of risk suggested by the letter, to identify the best way to respond (or not), and to be better prepared in case the C&D letter is followed by further (legal or non-legal) action by the sender. You may also find Section 4 ("FAQ on getting and working with an attorney") of this guide helpful.

3 What kinds of security research raise legal risk?

There are seven main areas of U.S. law that may raise legal risk for security researchers, as summarized in Table 1. The first column summarizes the main relevant areas of law, and the second column covers research activities that may create risks in those particular areas. It may seem counterintuitive, but the parts of your activity that carry legal risk often relate to low-level or mundane details rather than the more innovative aspects of your research.

Since multiple areas of the law may be relevant to any given research, be sure to read the second column carefully for all the different laws that might apply. Table 1 gives only a brief overview; for details, see the respective sections below (section pointers are in the left column).

The rest of this section is organized into subsections that overview each of the seven areas of law as they relate to security research. Some subsections include example scenarios and discuss how the law would apply to them.

Area of law	Potentially risky activities
The Computer Fraud and Abuse Act (CFAA) (§3.1) The CFAA is the federal anti-hacking / anti-computer-crime statute.	Accessing devices that you do not own, without the owner's permission
Copyright law (§3.2) Copyright law creates legal protections for "creative" works, including software.	Copying, modifying, or running software that you didn't write and do not have the permission of the copyright holder (often, the software author) to copy, modify, or run
Anti-circumvention provision of the Digital Millennium Copyright Act (DMCA §1201) (§3.3) The anti-circumvention provision prohibits bypassing certain access-control measures.	Circumventing measures designed to prevent or restrict access to software or other copyrighted works, such as encryption or password requirements
Contract law (§3.4) Contract law imposes liability for breaching a contract you agreed to.	Experimentation that violates a contract that you may have agreed to (including terms of use/service or non-disclosure agreements)
Trade secret law (§3.5) Trade secret law aims to protect confidential business information from misappropriation.	Using or disclosing information about software or a system design that a company keeps secret from a competitor
The Electronic Communications Privacy Act (ECPA) (§3.6) ECPA is a federal statute that aims to protect the privacy of electronic communications.	Collecting, observing, or analyzing third-party data flowing over a network
The Export Administration Regulations (§3.7) Federal law imposes certain conditions on publishing or transferring cryptography/security information and technology from the U.S. to abroad.	Transferring non-published information, code, or equipment related to cryptography to a foreign destination, outside the ordinary course of research. The government has never invoked export regulations against researchers; it seems highly unlikely they would do so absent very unusual circumstances.

Table 1: Potential areas of legal risk for security researchers

3.1 CFAA (Computer Fraud and Abuse Act)

The Computer Fraud and Abuse Act is the federal anti-hacking statute. It is quite broad, and encompasses many security research activities.

The broadest, most troublesome provision of the CFAA makes it illegal to "intentionally access a computer without authorization or exceed authorized access, and thereby obtain . . . information from" almost any computer. As the EFF said in its recent amicus brief to the Supreme Court, "[t]he CFAA does not define even its most critical terms: 'access' and 'authorization'—and in applying this unclear statute to today's world, some courts have diverged wildly from Congress' intent to stop serious computer break-ins" in a way that is harmful to security research.[8]

Currently, courts are divided about whether the statute's prohibition on "exceed[ing] authorized access" applies to people who have authorization to access data (for some purpose), but then access it for a (different) purpose that violates a contractual terms of service or computer use policy. Some courts have found that the CFAA covers activities that do not circumvent any technical access barriers, from making fake profiles that violate Facebook's terms of service to running a search on a government database without permission. Other courts, disagreeing with the preceding approach, have held that a verbal or contractual prohibition alone cannot render access punishable under the CFAA.

The Supreme Court has taken on a case, *Van Buren*,[9] which may rewrite much of this area of law and resolve some of the inconsistencies between different courts' approaches. So, if you're reading this after March 2021, there may be more clarity as to what the CFAA covers, and the information in this section may well be out of date.

Table 2 summarizes how the two main approaches taken by courts would treat different kinds of research activities, at the time of writing. While these two approaches summarize courts' behavior to date, bear in mind that the underlying reasoning of the courts does not generally commit to one approach or the other. This means that certain court decisions don't fit neatly into one category or the other, and future court decisions may diverge from these approaches, especially on cases of a new or unusual nature.[10]

[8] *See* Brief for Computer Security Researchers et al. as of Amici Curiae in Supp. of Pet'r, *Van Buren v. United States*, No. 19-783 (U.S. filed July 8, 2020), https://www.eff.org/document/van-buren-eff-security-researchers-amicus-brief.

[9] *United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019), *cert. granted*, 2020 WL 1906566 (U.S. 2020) (No. 19-783).

[10] Two recent examples are noteworthy. In 2019, the Ninth Circuit held that continuing certain research activities following a cease and desist letter is not a CFAA violation. *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019). In early 2020, the District Court in D.C. held that otherwise legal research that violates the terms of service of a consumer website is not a CFAA violation (although this case may yet be appealed). *Sandvig v. Barr*, No. 16-1368, 2020 WL 1494065 (D.D.C. Mar. 27, 2020). It is still unclear whether other courts would treat research that goes against the provisions of cease and desist letters or website terms of service as CFAA violations.

	Approach 1 (1st, 5th, 7th, & 11th Circuits)[11]	**Approach 2** (2nd, 4th, & 9th Circuits)[11]
Research that violates a binding contract[12]	Potential CFAA violation	No CFAA violation
Research involving only devices that you own, or devices whose owners have consented to the experimentation	No CFAA violation (unless the research violates a contract; see cell above)	No CFAA violation
Research involving devices (including remote servers) that you neither own nor have the owner's permission to experiment on[13]	Potential CFAA violation	

Table 2: Two main approaches to CFAA interpretation today

If you are working with devices that you don't own, whose owners have given permission for your experimentation, keeping a written copy of the permission (ideally, including specifics of the activity consented to) may help reduce your legal risk in case of a lawsuit. You may also want to be mindful of possible legal risk for the device owners, in case they've agreed to any contracts that prohibit them from giving such permission: in such cases, *you* would likely avoid CFAA liability if you had no reason to know of the contract violation, but the device owner might still be liable for breach of contract or other claims.

A CFAA violation can result in both civil and criminal liability. Civil lawsuits can be brought by any party harmed by the access, so long as they (can plausibly argue that they) have suffered $5000 of harm. In some jurisdictions, the cost of measures taken to investigate or respond to a computer intrusion count towards that number.

Finally, bear in mind that most U.S. states also have state-specific computer

[11] Circuits consist of groups of states, as shown in this map: https://www.uscourts.gov/sites/default/files/u.s._federal_courts_circuit_map_1.pdf [https://perma.cc/9S3R-K6E9].

[12] See also Section 3.4, below, which discusses when contracts are binding.

[13] This includes experimenting on your own account on someone else's machine (say, on a cloud platform), as well as connecting to websites hosted on servers you don't own (even if the website is yours), and using apps that (perhaps non-obviously) communicate with remote servers that you don't own.

Example 1 Testing hardware that doesn't belong to you

Suppose you want to test a home security system for vulnerabilities. The system requires a subscription for remote access, which comes along with a contract with a service provider that prohibits security testing and reverse engineering. A friend has the security system set up in their house, connected to their local network, and has offered to let you play with it.

The testing could run afoul of the CFAA for lack of authorization if you do not get clear permission from your friend in advance (ideally in writing) for the specific testing you want to do, or if you test beyond their local network (possibly accessing hardware whose owner has not given permission for the testing).

There can also be contract law considerations related to this kind of testing: see Section 3.4 below.

crime laws,[14] whose provisions may differ from the CFAA. This guide does not do a state-by-state analysis. If you are interested in analyzing potential legal risk under the laws of your state and any states whose laws your activity may fall under, you may wish to consult a lawyer.

3.2 Copyright law

Authors of software automatically own the copyright to any copyrightable portions of the code they write.[15] Making or distributing copies of software, or creating derivative software, may be a copyright violation unless *either* you have permission from the copyright owner *or* your copying falls within an exception under copyright law. Unfortunately, simply viewing or executing code may be found to constitute copying in some jurisdictions: some courts have stated that causing code to be copied from disk into RAM may count as making a copy for the purposes of copyright law.[16]

Even if you bought (or otherwise legally obtained) a copy of a piece of software, that doesn't necessarily mean you have permission to use it however you want. Most software (whether open-source or commercial) comes with a license describing how you are permitted to use it. Not all violations of a license create liability for copyright infringement. Only violations of "conditions," terms that are clearly explained as vital to being compliant with a license, potentially

[14] A summary of computer crime statutes is available here: http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

[15] Not all code is copyrightable, and determining which code portions are copyrightable can be complicated. However, given an entire piece of software, it is very likely to include some copyrightable material.

[16] *E.g.*, *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518 (9th Cir. 1993); *Quantum Sys. Integrators, Inc. v. Sprint Nextel Corp.*, 338 Fed. App'x 329, 336–37 (4th Cir. 2009). This interpretation has been widely criticized and some scholars have argued that RAM copies are fair use, but nonetheless, these decisions have not been overruled. See Christina Mulligan, *Copyright without Copying*, 27 Cornell J. of L. and Public Policy 469, 470-472 (2017).

exceed the scope of the license and can result in copyright infringement.[17]

Copyright infringement can lead to civil or criminal liability. For criminal liability, the infringement must be intentional and for the purpose of financial gain, whereas civil liability may apply even without a profit intent.

The Fair Use Doctrine

Fortunately, there is a defense to copyright infringement that may cover many security research activities: *fair use*.[18] Although there is no case law directly on the subject, the Copyright Office has suggested that using copyrighted works for good-faith security research is likely fair use.[19]

Courts determine whether a particular use qualifies as fair use by considering a number of factors on a case-by-case basis, with a view to promoting the "basic goal of copyright law: to put copyrighted works to their most beneficial use" for the public good.[20] No single factor is decisive. The following table summarizes the main factors that courts consider in their fair use decisions, along with examples of how courts may consider them. (But keep in mind that fair use determinations are highly dependent on the facts of each case, and none of these examples are iron-clad rules.) Overall, these factors would strongly favor a finding of fair use for most security research.

In many cases, if you use copyrighted material for a fair use, then any copies made in the process of achieving that fair use will be exempt from liability under the fair use doctrine (e.g., code copied for the purpose of running software in an emulator[21]). However, to reduce risk, it is still advisable to avoid making copies of software if there's an easy alternative that would still achieve your research goals.

---

[17] *See MDY Indus., L.L.C. v. Blizzard Entm't, Inc.*, 629 F.3d 928, 939 (9th Cir. 2010).

[18] 17 U.S.C. §107.

[19] Seventh Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention: Recommendation of the Acting Register of Copyrights 283, 298 (2018), https://www.copyright.gov/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf.

[20] *Wall Data Inc. v. L.A. Sheriff's Dept.*, 447 F.3d 759, 777 (9th Cir. 2006) (quoting The Federalist No. 43, at 257 (J. Madison) (New American Library ed. 1961) (1788)) (internal quotation marks omitted).

[21] *See Sony v. Connectix*, 203 F.3d 596, 604 (9th Cir. 2000).

	More likely to be found fair use	Less likely to be found fair use
Purpose	Nonprofit, educational, or academic; reverse-engineering to gain access to functional information[22]	Commercial (e.g., work for a paying client, creating software you'll charge for)
Type/character of use	"Transformative" use, i.e., different from the creator's primary intent or meaning[23]	Does not advance a new purpose or add new meaning (e.g., because it is similar to the original use)
Nature of copyrighted work	Less creative, more factual or functional (e.g., software, blueprints, or press releases)	More creative and expressive (e.g., novels, movies, or songs); unpublished
Extent of use	Using an amount reasonably necessary for / proportionate to the intended purpose[24]	Using an amount that is disproportionate to the intended purpose
Market impact	Use that doesn't directly compete with the original copyrighted work in its intended market[25]	Use that directly competes with the original copyrighted work or deprives it of its value[26]

Table 3: Fair use factors

[22] *See Sega v. Accolade*, 977 F.2d 1510 (9th Cir. 1992) (finding that copying and reverse engineering of video game console computer code by competitor for the purpose of releasing computer games for that console was fair use); *Sony v. Connectix*, 203 F.3d 596 (9th Cir. 2000) (holding that copying and reverse engineering of BIOS of Sony's video game console for the purpose of creating an emulation system was fair use).

[23] Security research is likely a "transformative" use, since in general, software is primarily intended to be executed rather than analyzed for vulnerabilities.

[24] Some copying is typically necessary to analyze software security, and moreover, publishing or sharing code snippets is reasonably necessary to explain the results of the research to the public or other interested parties. Limiting your publication of code snippets to the pieces of code that are directly relevant to explaining your findings may reduce your legal risk.

[25] Indirect impacts such as reputational harm to software creators because of vulnerabilities discovered in their code don't weigh against fair use.

[26] E.g., if you use copyrighted software to create other software that does the same thing.

Example 2 Analyzing and modifying functionality of software

Recall that you want to test a home security system for vulnerabilities. The security system contains a main control box and several small electronic doodads that are installed in windows to monitor whether windows are open or closed.

The window doodads communicate with the security system using a proprietary protocol. You examine the messages sent and received by the window doodads and figure out how the protocol works. You then reprogram a window doodad so that it always indicates that the window is closed.

This testing implicates copyright law because the protocol may be copyrightable, and you are copying, modifying, and/or creating a derivative work of the copyrightable code in order to test and reprogram the doodad. However, all three of these uses are almost certainly fair use, given that the use is transformative and there is no market harm via direct competition.

This example may also implicate DMCA §1201 and eavesdropping law, as discussed in Sections 3.3 and 3.6 below.

Example 3 Publishing code snippets in your research

Now suppose you want to publish a paper based on the research you did into the security of the home security system as discussed in Examples 1 and 2. A co-author suggests including snippets of the (potentially copyrightable) protocol that you investigated to illustrate how the programmers did not take basic security steps. In your paper, you criticize the choices made by the home security system company, including specifically those demonstrated by the code snippets you include.

Publication of copyrighted code implicates copyright law; however, using snippets of code for the purpose of commentary or criticism is likely a fair use under the statute. To limit legal risk, consider asking yourself whether each code snippet is relevant to the commentary or criticism you're making, and avoid including disproportionate amounts of code.

3.3 DMCA §1201 (Digital Millennium Copyright Act on circumvention)

One of the biggest legal barriers to security research generally is DMCA §1201, which prohibits the "circumvent[ion]" of "technological measures that. . . control[] access to"[27] copyrighted works, including software.[28] The DMCA does define some of these terms, although whether these definitions add clarity is questionable. For example:

[27] For completeness, we note that the word "effectively," which immediately precedes "control" in the quoted language, but has not been interpreted as meaningful. Even access controls that many security researchers would consider ineffective have counted under the statute - it is best not to put too much weight on a technology not "effectively" controlling access unless it literally does not work.

[28] For more information on how the DMCA anti-circumvention provisions have been used against researchers and others, see EFF's Unintended Consequences White Paper: https://www.eff.org/wp/unintended-consequences-under-dmca/archive.

- "to 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner;"[29] and

- "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[30]

Broadly speaking, §1201's anti-circumvention provision creates liability for removing or bypassing digital rights management on copyrighted works, as well as certain other types of access control mechanisms. §1201 liability can be either civil or criminal, although criminal liability under §1201 requires that a circumvention be "willful" and "for purposes of commercial advantage or private financial gain."[31] Although the language could be read to encompass security researchers, criminal prosecutions under §1201 have generally targeted commercial sellers of circumvention technology.[32]

Note that DMCA §1201 is not relevant unless technological measures control access to a copyrighted work. So circumventing a digital lock that met the definition above but did not restrict access to a copyrighted work would not violate the statute. [33] Therefore, digital rights management schemes that control access to *uncopyrightable* material (e.g., purely factual information)[34] or simply don't implicate any of the rights reserved to copyright holders (e.g., limiting access to a physical location) cannot create §1201 liability.

However, §1201 liability generally applies to circumvention of technological measures that control access to a copyrighted work even if the resulting access to copyrighted works is allowed under copyright law. In other words, §1201 prohibits circumventing access control mechanisms even if you don't infringe the copyright in the material they are meant to protect.[35] In particular, fair use (discussed in Section 3.2 above) does not apply as a defense to liability

[29] 17 U.S.C. §1201(a)(3)(A).
[30] 17 U.S.C. §1201(a)(3)(B).
[31] 17 U.S.C. §1204.
[32] *See, e.g., United States v. Silvius*, 559 Fed. Appx. 490 (6th Cir. 2014).
[33] *See, e.g., Lexmark Intern., Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004) (remanding to the trial court to consider whether a work subject to a §1201 claim was copyrightable).
[34] Generally, information may be copyrightable if it could be considered creative expression. Software is copyrightable, as are creative writing, artwork, and music. Purely factual data is generally not copyrightable (e.g., measurement data that a car/home/fitness device sends to the manufacturer), but factual data expressed in a creative manner is copyrightable (e.g., many news or encyclopedia articles). Some material that can only be expressed in one way may also not be copyrightable under the merger doctrine. We recommend consulting a lawyer to evaluate whether the information involved in a particular use case is copyrightable.
[35] *See MDY Indus., L.L.C. v. Blizzard Entm't, Inc.*, 629 F.3d 928 (9th Cir. 2010) (holding that no infringement nexus is required for §1201 liability). *But see also Chamberlain Grp., Inc. v. Skylink Tech., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004) (holding that an infringement nexus was required for §1201 liability).

under §1201, according to most courts: that is, you may be held liable for circumventing an access control even if you did so only to make a fair use of the copyrighted work it was protecting.

Fortunately, there are explicit exemptions to §1201 liability for good-faith security research. First, we discuss what kinds of activity are likely to be considered §1201 violations; then in the next subsection, we discuss the security research exemptions.

Courts have interpreted "technological measures that effectively control access" to encompass CAPTCHAs,[36] digital rights management (DRM) schemes (e.g., on DVDs and video games),[37] and software designed to deny game access to bots and players whose RAM reveals the presence of "cheats."[38] Courts have even debated whether "circumventing" rolling codes in garage door openers, or "circumventing" printer programs intended to prevent use of non-manufacturer-branded toner cartridges, could violate §1201; fortunately, the cases so far suggest not.[39] Software vendors have argued, or are likely to argue, that techniques such as authentication handshakes, code signing, and encryption all qualify as "technical protection measures" within the scope of the DMCA.

On the other hand, several courts have held that unauthorized use of a valid username and password does not violate §1201 (though at least one California court has disagreed).[40] A claim under §1201 (unlike under the CFAA) does not arise from unauthorized access alone, but from *circumvention* of digital protections on access to copyrighted materials. Some courts have reasoned that entering a valid username and password is not circumvention because it is the *intended manner* of access, even if used by an unintended party.[41] This question

[36] *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1111 (C.D. Cal. 2007) (treating CAPTCHAs as technological measures that effectively control access for DMCA purposes).

[37] *Sony Comput. Entm't Am., Inc. v. Divineo, Inc.*, 457 F. Supp. 2d 957 (N.D. Cal. 2006) (holding manufacturer of mod chips and software for making copies of PlayStation games liable under the DMCA for trafficking in devices designed to protect access to copyrighted material).

[38] *MDY*, 629 F.3d 928, 953–54 (imposing DMCA liability on the manufacturer of software that automatically played the early levels of World of Warcraft, and WoW included software designed to block bots and players using cheats).

[39] *See Lexmark Intern., Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004); *Chamberlain Grp., Inc. v. Skylink Tech., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004).

[40] *Compare I.M.S. Inquiry Mgmt. Sus. v. Berkshire Info. Sys.*, 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004) (defendant's unauthorized use of someone else's username and password, disclosed in violation of contractual obligation, did not qualify as circumvention under the DMCA); *R.C. Olmstead, Inc. v. CU Interface, L.L.C.*, 657 F. Supp. 2d 878, 889 (N.D. Ohio 2009) (a defendant does not "circumvent or bypass any technological measure" when he uses "the approved methodology," such as a user name and password, to access copyrighted material); *Egilman v. Keller & Heckman, L.L.P.*, 401 F. Supp. 2d 105 (D.D.C. 2005); *Burroughs Payment Sys., Inc. v. Symco Grp., Inc.*, 2011 WL 13217738, at *4–*6 (N.D. Ga. Dec. 13, 2011); *Navistar, Inc. v. New Baltimore Garage, Inc.*, 2012 WL 4338816, at *5 (N.D. Ill. Sept. 20, 2012), *with Actuate Corp. v. International Business Machines Corp.*, No. 09–CV–5892, 2010 WL 1340519 (N.D.Cal. April 5, 2010) (holding that the use of passwords "without authorization" is no different than the unauthorized use of other technologies to gain access to copyrighted material, and therefore it "avoids and bypasses a technological measure in violation [of the DMCA.]").

[41] *See Dish Network L.L.C. v. World Cable Inc.*, 893 F.Supp.2d 452, 467-468 (E.D.N.Y.

has not arisen in all jurisdictions, and given the relative scarcity of precedent, it's hard to say what other courts will decide or how far they would extend this reasoning to other situations.

Purely physical protection measures (e.g., a padlock) also seem unlikely to be considered "technological measures" under DMCA §1201, because the overall context and language of the DMCA strongly suggest an intent to target digital activity. However, no court has yet considered this question directly.

DMCA §1201(a)(2) and §1201(b)(1) additionally prohibit trafficking in technology that is primarily designed, marketed, or valuable for circumvention of access or "copy" controls. Trafficking could mean distributing (commercially or not) or otherwise facilitating trade in such tools. Generally available tools (such as soldering irons, screwdrivers, software-defined radios, Google, hardware debuggers, etc.) have commercially significant purposes other than circumvention and are not marketed primarily for use in circumvention, so they are unlikely to trigger §1201 anti-trafficking liability. However, more specialized tools may create liability: for example, penetration testing tools, especially those that are primarily marketed or designed for circumvention of security protections on systems and/or those that automate testing (such as, arguably, WiFi Pineapples, Bash Bunnies, Metasploit, or Kali Linux).[42] Before releasing or distributing tools that allow such circumvention, you should consult with an attorney.

The next subsections describe exemptions to DMCA liability that apply to both the anti-circumvention provision and the anti-trafficking provisions. Given the breadth of the DMCA, it is fortunate that there are some exemptions! There are two types of exemptions to the DMCA: permanent exemptions and temporary exemptions.

Permanent security research exemptions

There are a small number of permanent exemptions that may apply to some security research activities. If an activity fits under a permanent exemption, that is preferable to a temporary exemption, as only the permanent exemptions eliminate liability under the anti-trafficking provisions as well as the anti-circumvention provisions. However, it is worth noting that the permanent exemptions have never been successfully invoked as defenses in court and rarely have been invoked at all. This does not mean they do not protect researchers, but it does mean we have to draw mostly on the text of the statute rather than case law.[43]

2012) (discussing how the statute should be construed to not cover intended manners of access).

[42] None of these examples have actually been tested in court. It is possible that a court would find that tools for security testing do not necessarily count as being primarily marketed for the purpose of circumvention, or that the permanent exemption (discussed below) applies.

[43] *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (rejecting a §1201(j)(4) exemption defense).

Security testing. §1201(j)(4) exempts certain forms of security testing from §1201 liability, including some forms of anti-trafficking liability.[44] It is this exemption to the anti-trafficking provisions that allows for certain forms of security testing tools to exist.

In order to take advantage of this exemption, testing must be done with "with the authorization of the owner or operator of such computer, computer system, or computer network."[45] This means that research where a researcher does not acquire permission is not covered by this exemption.

Encryption research. §1201(g) exempts certain forms of encryption research from §1201 liability: specifically, investigation of encryption technologies applied to copyrighted works.[46] The plain language of the exemption seems to apply broadly, although some lawyers interpret it as only covering encryption research on DRM.

Unlike the security testing permanent exemption, this exemption requires only that a researcher has "made a good faith effort to obtain authorization before the circumvention."[47] In determining whether this exemption applies to a given situation, factors to be considered include: whether the research was conducted in such a way as to "advance the state of knowledge and development of encryption technology" as opposed to "facilitat[ing copyright] infringement;" whether the researcher is "engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology;" and whether and when the researcher informs the copyright holder about the research.[48]

Temporary security research exemptions

The 2018 security research exemption[49] allows for circumvention of technical measures to access computer programs on lawfully acquired devices or machines, so long as the circumvention is otherwise lawful and is conducted solely for the purpose of good-faith security research. It is significantly broader than the two permanent exemptions.

More specifically, the 2018 exemption exempts from liability any circumvention that (1) is "undertaken on a lawfully acquired device or machine on which the computer program operates, or is undertaken on a computer, computer system, or computer network on which the computer program operates with the authorization of the owner or operator of such computer, computer system, or computer network, [(2)] solely for the purpose of good-faith security research and [(3)] does not violate any applicable law, [including the CFAA.]"

[44] 17 U.S.C.A. §1201(j).
[45] 17 U.S.C.A. §1201(j)(1).
[46] 17 U.S.C.A. §1201(g).
[47] 17 U.S.C.A. §1201(g)(2)(C).
[48] 17 U.S.C.A. §1201(g)(3).
[49] 37 C.F.R. §201.40(b)(11).

Two especially ambiguous terms stand out in this language: "lawfully acquired device" and "solely for the purpose of good-faith security research." Given the recency of the exemption at the time of writing, there are no cases illustrating how exactly courts will interpret these terms. However, below we discuss what the terms are likely to mean.

"Lawfully acquired" It is likely that both purchasing devices from a manufacturer and purchasing them or receiving them as gifts from third parties would be considered lawful acquisition. Receiving devices on loan may not be considered acquisition at all (so when testing loaned machines, the relevant question would be whether its owner lawfully acquired it). Indicia that a transaction or seller is not above board may make it more difficult to argue that a device is lawfully acquired. Given the uncertainty with regards to lawful acquisition, it is better to receive explicit authorization (ideally in writing) from the owner or operator of a device to engage in the relevant testing.

"Solely for the purpose of good-faith security research" The security research exemption specifies some criteria necessary to be considered good-faith security research.

1. The research must be done in an environment designed to avoid any harm to individuals or the public.

2. Information derived from the activity must be used primarily to promote the security or safety of the class of devices or machines on which the copyrighted program operates, or the people who use them.

3. Information derived from the activity must not be used or maintained in a manner that facilitates copyright infringement.

Courts may also consider other circumstantial factors when determining whether a particular activity counts as good-faith security research. Following coordinated disclosure practices, if possible, can weigh in a researcher's favor, although the exemption does not require it.

The 2018 security research exemption is valid for three years and will be up for renewal in 2021. If renewed, the language and scope of the exemption may also be revised in 2021. (There were significant changes between the 2015 and 2018 versions, which were favorable in that the 2018 version exempts a wider class of research activities.)

3.4 Contract law

Generally, the kinds of contracts that security research might violate fall into three broad categories.

1. **EULA.** Most software today comes with contracts called *end-user license agreements* that describe how users may use the software.

Example 4 Examining or modifying proprietary software

Recall that you want to test a home security system for vulnerabilities. The system contains window doodads that communicate with the security system using a proprietary protocol. As in Example 2, you examine the messages sent and received by the window doodads and figure out how the protocol works; you then reprogram a doodad so that it always indicates that the window is closed.

This research implicates §1201 because certain types of proprietary protocols may be copyrightable, and courts may consider any measures that the company took to obscure how their protocol works (even if they are easy to bypass) to be technological protection measures under the statute.

Examining a protocol without modifying it or bypassing any security features does not violate §1201. In other words, simply figuring out how to circumvent an access control measure without taking any concrete steps towards circumventing it does not count as "circumvention" under §1201.

On the other hand, reprogramming a device to eliminate security checks may count as circumvention. However, even if your actions were considered circumvention, you would not be liable under §1201 as long as your project is good-faith security research covered by the 2018 exemption (discussed above).

2. **TOS/TOU.** Many websites, app stores, devices, and other Internet services come with contracts called *terms of service* or *terms of use*.

3. **NDA.** Researchers may receive access to code or information pursuant to a *non-disclosure agreement*, developer agreement, or API agreement that restricts the ways they can report or publish about security flaws.

When assessing what contractual legal risk applies to your planned research, you should consider what EULA/TOS/TOU contracts are attached to the hardware, software, and services you plan to use, and whether you signed any NDAs or similar agreements. For each contract you identify as potentially relevant, there are three main questions to consider.

1. Am I bound by the contract?

2. If so, would my activity violate the specific terms of the contract?

3. If so, what sorts of liability or other consequences could result?

The following subsections briefly discuss the three questions in turn.

Am I bound by the contract?

Contract law varies by state. This section describes the most common approaches to contract enforceability, but to understand the details of your state's specific approach, you should consult a lawyer.

In general, boilerplate "take it or leave it" agreements like EULA/TOS/TOUs are less likely to be enforced as valid contracts than NDAs, developer agreements, and the like. The latter types of agreement are usually enforced, which

relates to the idea that they are more negotiable (in principle) and deliberately entered into.

Website TOS/TOUs are often enforced even if you didn't read them. But they will generally not be enforced against individuals if they did not have meaningful notice of the terms: e.g., if the website did not prompt them to read the terms, or if the terms (or a link to them) are buried in an inconspicuous part of the webpage.

Even if a contract states that its terms may be changed unilaterally (with or without notice), changed terms will generally not be considered binding unless you have been notified of the change.[50]

Would my activity violate the contract terms?

Of course, the answer to this question depends on the contract and on the contract law of the state in question. A useful place to start is to read your contract terms carefully. You may wish to consult a lawyer to determine the detailed scope of your contractual obligations. This section briefly discusses a couple of particularly relevant types of contract terms.

"No reverse engineering" clauses. Some contracts explicitly prohibit reverse engineering. These clauses are likely to be interpreted broadly as prohibiting any kind of analysis that aims to improve one's understanding of how the target software/hardware operates, or to create a similar or modified version of its functionality. Such provisions are generally enforceable, although any recovery against a researcher would be limited to the value of the contract.

Bug bounties and vulnerability disclosure programs. Although companies with bug bounty and vulnerability disclosure programs may give the impression of endorsing security research on their products, the existence of such programs does not prevent a company from taking legal action against you for security research activities, unless they are accompanied by a safe-harbor program in which the company commits not to take legal action. The Disclose.io Safe Harbor project maintains a useful list of public bug bounty programs[51] and whether they offer safe harbor. Ambiguous terms as part of a bug bounty program's safe harbor may decrease their usefulness, although a court may impose a duty to act in good faith in interpretation of the contract.

What liability (or other consequences) could result?

If someone breaches a contract, the other parties can seek *damages* (i.e., monetary compensation) from the breaching party. The amount of damages may

[50] *Online Contracts: We May Modify These Terms at Any Time, Right?*, American Bar Association: Business Law Today (May 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/05/07_moringiello [https://perma.cc/62YJ-APSN].

[51] https://www.bugcrowd.com/bug-bounty-list

be set out explicitly in the contract.[52] If not, the aggrieved party or parties can seek "compensatory damages," the amount of which is determined by a judgment of how much harm the breach caused.

For EULAs that grant you a license to use software, breaching the EULA conditions can result in that license being revoked (in addition to, or instead of, liability in the form of damages). Continuing to use the software after violating the EULA could open you up to a copyright infringement claim—although if your use of the software is limited to security research, you may not be liable (as discussed in more detail in Section 3.2 above).

Often, software vendors, website owners, and others will not go through the expense and inconvenience of bringing a lawsuit for a breach of TOS/TOU/EULA, especially because the damages for minor breaches of contract would typically be small even if they win. Aggressively bringing lawsuits against individuals may also damage their reputation. More often, upon discovering a breach, the software vendor or website owner might simply disable your account, cancel your subscription, or employ technical measures designed to block your access to their software/service. In rare cases, however, they could consider it worthwhile to sue despite expecting to lose money (or even to lose the case) in hopes of deterring future similar activity or publication of an embarrassing story about their vulnerability. The prominence of the breaching organization or individual might influence a decision to sue or not to sue in such a case.

Finally, as mentioned above in Section 3.1, there is some legal uncertainty around whether certain contract violations can additionally trigger criminal liability under the CFAA. However, it seems unlikely that contract violations in the course of otherwise legal security research would be prosecuted in practice (absent some other motive for prosecution, e.g., other crimes being involved), as discussed in more detail in Section 3.1.

Example 5 Contracts you haven't seen or (even nominally) agreed to

As in the previous Examples, you want to test a home security system for vulnerabilities. The system requires a subscription for remote access, which comes with a contract with a service provider that prohibits security testing and reverse engineering. A friend has the security system set up in their house, connected to their local network, and has offered to let you play with it. You do not see or agree to any terms of service for the security system, although your friend has. Because you are not a party to the contract (your friend agreed to the terms for the system, not you), you cannot be liable for breach of contract, although you may be liable under other bodies of law.

[52] E.g., a contract might say explicitly, "if either party breaches this contract, they will pay the other party $100." State law will determine whether the provision is enforceable.

Example 6 Contracts to which you've arguably indicated assent

Same as Example 5, but suppose you additionally download a software package from the home security system company's website, in order to use the management interface on a new computer. When installing the software, you click through the installation steps, including clicking "I agree" or "OK" on a screen displaying the terms and conditions for using the software. Unlike in Example 5, you could potentially be liable for breach of contract.

3.5 Trade secret law

Trade secret is a form of legal protection for information that is not known by the general public and confers an economic advantage on the holder. Trade secrets are protected by both state and federal law.

Trade secrets may cover some aspects of how software works meaning that "misappropriating" it could carry a civil or criminal liability. We won't get into the definition of misappropriation here, but just note that reverse engineering generally is *not* misappropriation unless it violates an NDA or similar (contractual) obligation.[53] Section 3.4, above, may help you think through whether you are under a contractual obligation not to reverse engineer some software. If you are able to do security research without inside information about a piece of software—that is, information that the company or its employees gave to you in a non-public way—then trade secret law is unlikely to apply.

3.6 ECPA (Electronic Communications Privacy Act)

In relevant part, the Electronic Communications Privacy Act (ECPA)[54] prohibits interception of electronic communications flowing over a network without the consent of a party to the communication. Under ECPA, the consent of any single party to the communication suffices (even if other parties to the communication do not consent).[55] Violating ECPA can give rise to civil or criminal liability.

Because packets are communications, network packet inspection may constitute "interception" under ECPA, especially on wifi networks that are unencrypted, and even if you only retain metadata such as addressing information.[56] Interception must be contemporaneous to create liability under ECPA; information at rest generally does not trigger ECPA liability.[57]

Courts have not squarely confronted the issue of who counts as a party under

[53] *Kewanee Oil Corp. v. Bicron Corp.*, 416 U.S. 470 (1974); 18 U.S.C. §1839(6)(B) ("[T]he term 'improper means' . . . does not include reverse engineering . . . ."); Cal. Civ. Code §3426.1(a) ("Reverse engineering or independent derivation alone shall not be considered improper means.").

[54] 18 U.S.C. §§2510–2523.

[55] 18 U.S.C. §2511(2)(c).

[56] *Joffe v. Google, Inc.*, 746 F.3d 920, 926 (9th Cir. 2013).

[57] *Compare United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010) *with United States v. Steiger*, 318 F.3d 1039 (11th Cir. 2003).

ECPA. That is to say, it is unclear whether an intermediary who transmits information (such as a wifi network owner or Mail Transfer Agent) can to grant consent for the purposes of ECPA.[58]

To minimize legal risk, consider limiting any packet inspection to communication to which you are a party, or where one of the parties to the communication has given you consent. In the latter case, keeping a copy of written consent (with a clear description of the research activities consented to) may help to further minimize risk.[59]

Finally, bear in mind that most U.S. states also have state-specific eavesdropping laws,[60] whose provisions may differ from ECPA. Some states require the consent of all parties to a communication under certain circumstances; however, many of these states don't specifically discuss electronic communications. This guide does not do a state-by-state analysis. If you are interested in analyzing potential legal risk under the laws of your state and any states whose laws your activity may fall under, you may wish to consult a lawyer.

Example 7 Packet inspection in transit and at rest

Suppose your colleagues are messaging each other online (whether encrypted or not). Under ECPA, you would not be liable for inspecting their messaging packets as long as you had permission from at least one of them, but you could potentially be liable if you permission from none of them. (If you were a party to the messaging too, then note that your own permission would suffice.)

In contrast, examining the message data at rest on a device is outside ECPA's scope (which covers in-transit communication), so cannot trigger ECPA liability regardless of others' permissions. Examining a device without the device owner's permission may, of course, raise other (non-ECPA) legal issues.

3.7 Export controls

In theory, federal law imposes certain conditions on publishing or transferring from the U.S. to abroad certain software, hardware, or information related to encryption and information security.[61] A list of things restricted for export, including certain things related to encryption/security, is also agreed upon (and annually revised) by dozens of countries that each implement corresponding domestic-law restrictions—so other countries may have similar restrictions.[62]

[58] *See, e.g.*, *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 844–45 (N.D. Cal. 2017). Sensibly, there is an exception that means that such intermediaries are generally not subject to ECPA liability themselves for handling such communications in their role as intermediaries.

[59] *In re Google Inc. Gmail Litig.*, Case No. 13-MD-02430-LH, 2014 WL 1102660 (N.D. Cal. 2014) (discussing methods of obtaining consent for exception to wiretap act to apply).

[60] See this summary of state computer crime statutes for more information: http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

[61] *See, e.g.*, 15 C.F.R. §§730–74.

[62] Wassenaar Arrangement Secretariat, *List of Dual-Use Goods and Technologies and Munitions List* (Dec. 2019), https://www.wassenaar.org/app/uploads/2019/12/WA-

In practice, the government has never enforced these laws against researchers (over two dozen years of their existence), and has suggested that it would not want to do so.[63] Technically, however, violating these conditions could result in severe criminal penalties, and the restricted conduct includes some commonplace research activities.

This is, of course, an incredibly frustrating situation. The laws have been challenged in court, with encouraging results; however, courts indicated that they may not issue an iron-clad clarification until confronted with a case involving credible risk of prosecution.[64] In the years since these court challenges, new provisions of the regulations have placed certain kinds of research activity more clearly outside the scope of export control rules.

Next, we summarize the cryptography-related requirements of the Export Administration Regulations[65] (EAR) at the time of writing, at least as they appear on paper. As noted above, (some of) these rules are routinely broken by researchers, and *it seems very unlikely that a researcher would be penalized for such activity*. We include this summary for informational purposes, and for completeness, rather than to suggest these activities carry significant legal risk.

DOC-19-PUB-002-Public-Docs-Vol-II-2019-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-19.pdf; *About us*, The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies, https://www.wassenaar.org/about-us [https://perma.cc/4F6W-6MLU].

[63] In a 2002 court hearing, a Justice Department attorney apparently "assure[d]" the court that "the regulatory authority does not want [researchers who are collaborating at conferences] sending us an e-mail every time they change something in an algorithm" and gave "repeated assurances" that a computer security researcher was "not prohibited from engaging in" any of his proposed research activities. Daniel J. Bernstein, *Crypto Case on Indefinite Hold (Oct. 2003)*, https://cr.yp.to/export/2003/10.15-bernstein.txt. Footnote 64 gives more context about this case, the final one in a series of cases by Daniel J. Bernstein.

[64] Daniel J. Bernstein, then a Ph.D. student at U.C. Berkeley, brought a constitutional challenge to certain aspects of the export restrictions in 1995, represented by EFF. Around the same time, Peter Junger, a professor of computer law, challenged the restrictions in Ohio. Both the Sixth Circuit and the Ninth Circuit issued decisions finding that the requirement of pre-publication approval by the government was an unconstitutional violation of First Amendment free speech rights, and invalidating the corresponding provisions of the export regulations. *Bernstein v. U.S. Dep't of Justice ("Bernstein I")*, 176 F.3d 1132 (9th Cir. 1999); *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000). This was a win for Bernstein, Junger, and security researchers (although many aspects of the export restrictions still remained intact).

The Ninth Circuit decision is not legally binding precedent, due to the complicated history of the Bernstein case, which is summarized next for curious readers. A three-judge panel of the Ninth Circuit initially held the requirement of pre-publication approval to be unconstitutional in *Bernstein I*. However, the Ninth Circuit subsequently granted the government's request to have the case reheard by all eleven judges of the Ninth Circuit (technically "withdrawing" the prior three-judge decision), and then due to changes in the export regulations, the rehearing never happened—technically leaving the case without a legally binding decision, though *Bernstein I* remains instructive. *Bernstein v. U.S. Dep't of Justice ("Bernstein II")*, 192 F.3d 1308 (9th Cir. 1999); *see also Bernstein v. U.S. Dep't of Commerce ("Bernstein IV")*, 2004 WL 838163 at *2 n.2 (N.D. Cal. 2004). Bernstein's follow-up case in 2002, challenging the new regulations, was dismissed on the grounds that his proposed research activities were "not prohibited" and he could come back to court "[i]f and when there is a concrete threat of enforcement against [him] for a specific activity." Daniel J. Bernstein, *Crypto Case on Indefinite Hold (Oct. 2003)*, https://cr.yp.to/export/2003/10.15-bernstein.txt.

[65] 15 C.F.R. §§730–74.

If you are considering transferring some information, software, or hardware from the U.S. to abroad and are curious whether such transferral is permitted under the EAR, here are the two main possibilities.

1. ***Are you considering publishing encryption source code?*** If so, the law technically requires you to notify the Department of Commerce and the NSA.[66] If you would like to follow this requirement, simply email crypt@bis.doc.gov and enc@nsa.gov with either a copy of or a link to the code. Technically, if you send a copy of the code, you are required to notify them again each time the "cryptographic functionality" of the code changes; or if you send a link, then you don't need to notify them of changes to the code, but you are required to notify them of URL changes. Once some encryption source code is published and the requisite notification made, the EAR no longer impose any restrictions on distributing that source code or any corresponding compiled code abroad.[67]

2. ***Are you considering transferring information or software abroad in one of the following four categories exempt from the EAR?*** If so, your activity is permitted under the EAR. (However, to the extent that you are publishing encryption source code, the notification requirement described in the preceding bullet still applies.)

   The four exempt categories. Information and software is exempt from the EAR (though possibly still subject to the notification requirement described in Question 1 below) if it satisfies any of the following conditions:[68]

   - it is "published;"[69]
   - it "arise[s] during, or result[s] from, fundamental research;"[70]
   - it is "released by instruction in a catalog course or associated teaching laboratory of an academic institution;" or
   - it "appear[s] in patents or open (published) patent applications. . . unless covered by an invention secrecy order."

Sending information, code, or systems from the U.S. to abroad, if it does *not* fall under exceptions such as listed above, may be restricted or prohibited

[66] 15 CFR § 742.15(b).
[67] *See, e.g.*, 15 C.F.R. § 734.17(b)(2).
[68] 15 C.F.R. §734.3(b)(3).
[69] "Published" is defined liberally to include: paywalled publication; availability at public libraries; presentation at a "conference, meeting, seminar, trade show, or exhibition" that is "generally accessible to the interested public;" and communication of manuscripts, presentations, and related information to co-authors, other researchers, and reviewers "with the intention that such information will be made publicly available if accepted for publication or presentation." 15 C.F.R. §734.7.
[70] "Fundamental research means research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons." 15 C.F.R. §734.8.

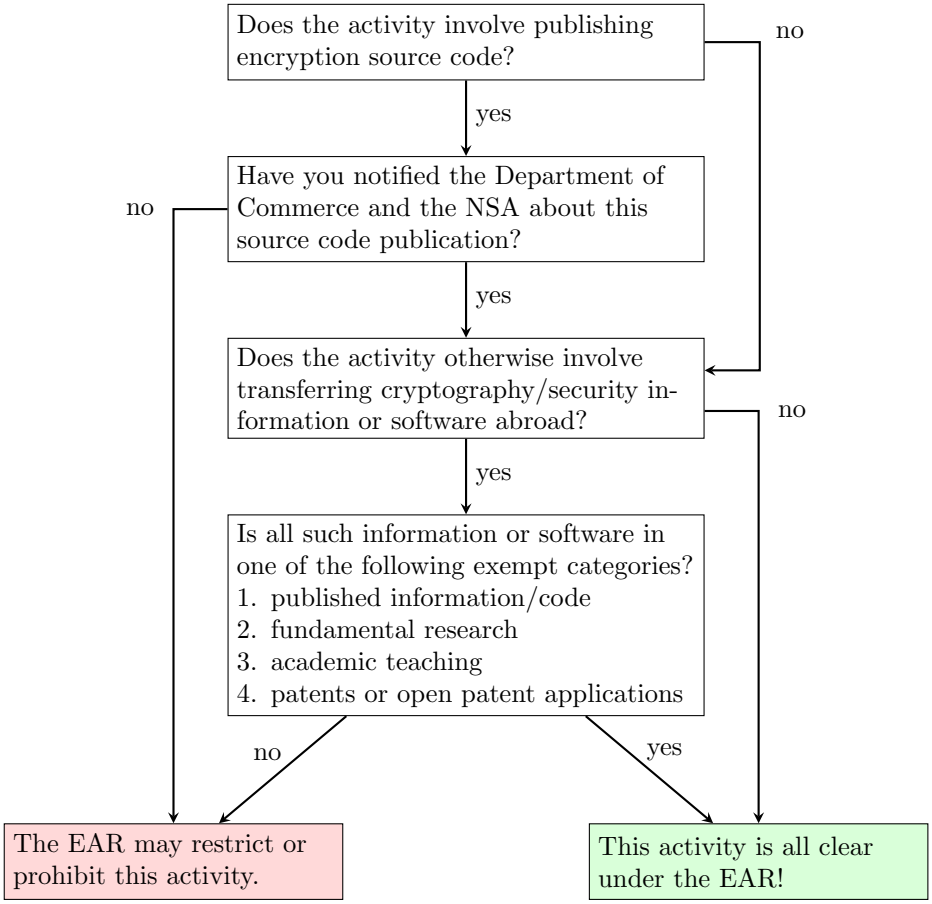

Figure 1: Some exemptions to the Export Administration Regulations

by the EAR.[71] These considerations are summarized graphically in Figure 1.

If you are violating export control rules in a context that is outside the ordinary course of research and could plausibly raise non-trivial concerns that the information would then be used against the United States by a foreign power, you may want to consult a lawyer about your legal risk.

Finally, universities often have (possibly obscure) rules or advice about the sort of activity regulated under export control laws.[72] University researchers

[71] The EAR do not necessarily prohibit these activities outright: for example, you may be permitted to sell products to the mass market if you get a license and/or send the government regular reports.

[72] *See, e.g.*, *Export Control Policies & Procedures*, Harvard University: Office of the Vice Provost for Research, https://vpr.harvard.edu/pages/export-controls-policies-and-procedures [https://perma.cc/4B3W-55SB]; *Export Control*, MIT: Office of the Vice President for Research, https://research.mit.edu/integrity-and-

may be curious to check what their university's policies say.

4 FAQ on getting and working with an attorney

Despite what may seem like frequent suggestions to consult a lawyer, we don't actually think that all security researchers need an attorney on speed dial. Often, you'll be just fine without a lawyer's input. But depending on the situation, it may be very helpful to have a lawyer: one of this guide's aims is to help you make informed decisions regarding whether and when to get one, and if so, how. To that end, this final section discusses some common questions and concerns about getting a lawyer.

We talk about this in detail because "lawyering up" can feel daunting or off-putting. And it's true that sometimes working with a lawyer can be a crappy experience. But it doesn't have to be! There are lawyers who work with security researchers and can provide advice that helps minimize your risk while allowing you to accomplish your goals.

This section tries to address some commonly asked questions.

Does talking to a lawyer make me look like I'm guilty of something or increase my risk?

Generally, no. Speaking to an attorney helps you better understand any risks that you are taking, as opposed to increasing them. While there might be some unusual edge cases where it can be better to not know what you are getting yourself into, in the vast majority of cases you will be better off understanding the legal landscape you are facing. Lawyers may be able to suggest ways to decrease your risk without changing your research. In addition, attorneys are bound by professional ethical obligations to not share information you share with them in the course of a legal representation with anyone else. So you can talk about what you're thinking about without worry that the attorney will pass on the information. Much as security through obscurity is not a good game plan, avoiding lawyers won't protect you from the law!

Where can I find a lawyer who knows about security research?

Great question! Our suggestion would be to reach out to EFF or the Cyberlaw Clinic, either of which can help you find representation. It is common for attorneys to help locate a lawyer for someone even if they cannot help that person themselves.

What can I expect from my first conversation with an attorney?

Generally, an attorney will spend the first conversation getting to know you and your work and plans. They may ask about your research, about

compliance/export-control [https://perma.cc/QY2C-2KBG]; *Strong Encryption Export Controls*, Stanford University: Office of the Vice Provost and Dean of Research, http://web.stanford.edu/group/export/encrypt_ear.html [https://perma.cc/NDU6-AMWY].

your publication plans, or about any past experiences you have had with legal threats. Even some attorneys who work in private firms will do an initial consultation for free as part of helping to scope future representation. If money is an issue and you aren't able to procure pro bono (free) legal counsel, it may be possible to ask for a limited representation or conversation that covers one particular issue you are worried about.

What if I don't like my attorney or find working with them difficult? What if they tell me not to do certain research?

An attorney's advice is just that, advice. Ultimately, the decision of how to proceed is up to you as the client. If you don't like your attorney or find working with them difficult, it is totally reasonable to find someone else to work with or make a decision as to your own personal risk that your lawyer does not agree with.

Isn't getting a lawyer incredibly expensive?

Although lawyers can charge a lot of money, there are attorneys who are willing to help out individuals and academic researchers for free or for low cost. In addition, if you work with an attorney who is experienced in this practice area, it will take them less time to give you helpful advice to reduce your risk (which means less cost for you, since lawyers typically charge by the hour).

My university/employer/friend has an attorney. Can I just listen to them?

Although sometimes it can be valuable to consult with an attorney that represents someone else, they may not be able to give you individual advice or may be obliged to give advice that is more tailored to reducing the institution's risk or otherwise more tailored to the institution's interests than your own. It is also worth noting that some institutional attorneys (such as university general counsels) may not understand security research and so may assume that any legal risk taking means the research is ill-advised. It's always best to have an attorney who works with you individually!

Why do all these lawyers say that they're not my lawyer and not giving me legal advice?

It's annoying, right? Many lawyers will say that they're not giving legal advice because they do not want to accidentally create a lawyer/client relationship. Because lawyers have professional ethical obligations with respect to their clients,[73] it's in all parties' interest to be careful that friends, colleagues, and random people on the Internet don't think an attorney is representing them when they're not, and don't think that an attorney is giving "legal advice" tailored to their specific situation and

[73] Some examples include: confidentiality, certain kinds of disclosures, avoiding conflicts of interest, and "zealous representation."

researched exhaustively (as in a lawyer/client relationship) when actually the attorney is speaking in more general terms.

5 Conclusion

This guide provides an introduction to some legal issues that might affect security researchers, and what research activities tend to be more or less risky.

It's reasonable to be intimidated or put off by the multiple, often ambiguous bodies of law that may apply to security research. Especially in a fast-changing context like technology, it is typical for the law to remain unclear on edge cases until tested by litigation. For better or worse, there hasn't been much litigation so far, and in some of these areas, it's difficult to get clarity without litigation. Given the importance of security research in improving the technologies that increasingly pervade our lives, it seems possible that courts may become more sympathetic to security research and researchers than they have been in past cases. In the meantime, especially in a landscape of legal uncertainty, it's not all about jumping through legalistic hoops: bear in mind that it will often reduce your legal risk to conduct your research in ways that are aligned with widely accepted norms in the field and be respectful of the interests of others who might be impacted by your research. In short, don't be an idiot.

If you are planning research and are worried about liability, it's good to consider consulting an attorney. Both EFF and the Cyberlaw Clinic provide some pro bono (free) service to security researchers, and may be able to find counsel for researchers whom they are not able to work with directly: email info@eff.org and/or fill out the Clinic's intake form[74] to inquire.

[74] http://blogs.harvard.edu/cyberlawclinic/clients/potential-clients

6 About the authors

Sunoo Park is a J.D. candidate at Harvard Law School and a cryptography and security researcher. Before law school, she completed her Ph.D. in computer science at MIT. As a student in the Cyberlaw Clinic at Harvard Law School, Sunoo worked with Kendra on legal issues impacting security researchers: that was the beginning of a series of discussions that led eventually to this Guide.

Kendra Albert is a clinical instructor at the Cyberlaw Clinic, where they teach law students to practice technology law by working with pro bono clients. Prior to starting at the Cyberlaw Clinic, they worked with Marcia Hofmann at Zeitgeist Law, primarily working with security researchers. They are licensed in Massachusetts and California.

The Cyberlaw Clinic at Harvard Law School, based at the Berkman Klein Center for Internet & Society, provides pro bono legal services at the intersection of technology and social justice. The Cyberlaw Clinic was the first of its kind, and it continues its tradition of innovation in its areas of practice. The Clinic strives to center clients in its legal work, helping them to achieve success as they define it, mindful of (and in response to) existing law.

The Electronic Frontier Foundation (EFF) is a nonprofit civil liberties organization that has worked for over 30 years to protect innovation, free expression, and civil liberties in the digital world. As part of its Coders' Rights Project, EFF offers pro bono legal services to researchers engaged in cutting-edge exploration of technology whose work in the public interest may be unjustly chilled. EFF's ***Andrew Crocker***, ***Cara Gagliano***, ***Kurt Opsahl***, and ***Kit Walsh*** were instrumental to editing this Guide.

Acknowledgments

We are grateful to Hal Abelson, Ross Anderson, Aisling Connolly, Joseph Lorenzo Hall, Bruce Schneier, Michael Specter, and Tarah Wheeler for helpful conversations and reviewing draft versions.