COLORADO LAW
UNIVERSITY OF COLORADO LAW SCHOOL

LEGAL STUDIES RESEARCH PAPER SERIES

Working Paper Number 07-14
May 22, 2007

The Myth of the Superuser: Fear, Risk, and Harm Online

Paul Ohm
University of Colorado Law School

UC DAVIS
LAW REVIEW

UNIVERSITY OF CALIFORNIA, DAVIS, SCHOOL OF LAW • VOL. 41, NO. 4, APRIL 2008

The Myth of the Superuser: Fear, Risk, and Harm Online

Paul Ohm[*]

Fear of the powerful computer user, the "Superuser," dominates debates about online conflict. He is a mythic figure: difficult to find, immune to technological constraints, and aware of legal loopholes. Policymakers, fearful of his power, too often overreact by passing overbroad, ambiguous laws intended to ensnare the Superuser but which are instead used against inculpable, ordinary users. This response is unwarranted because the Superuser is often a marginal figure whose power has been greatly exaggerated.

The exaggerated focus on the Superuser reveals a pathological characteristic of the study of power, crime, and security online, which springs from a widely held fear of the Internet. Building on the social science fear literature, this Article challenges the conventional wisdom and

[*] Associate Professor of Law and Telecommunications, University of Colorado Law School. Thanks to Tim Wu, Orin Kerr, Phil Weiser, Julie Cohen, Pierre Schlag, Brett Frischmann, Victor Fleischer, Miranda Fleischer, Viva Moffat, and Jean Camp for their helpful comments. Thanks also for suggestions and support from participants in the University of Colorado Law School Faculty Workshop, including Clare Huntington, Nestor Davidson, Scott Peppett, Mimi Wesson, Amy Schmitz, Sarah Krakoff, and Brad Bernthal; the Intellectual Property Scholars Conference; and the Telecommunications Policy Research Conference. Thanks also to Todd Blair and Michael Beylkin for outstanding research assistance.

standard assumptions about the role of experts. Unlike dispassionate experts in other fields, computer experts are as susceptible as laypeople to exaggerate the power of the Superuser.

The experts in computer security and Internet law have failed to deliver us from fear, resulting in overbroad prohibitions, harms to civil liberties, wasted law enforcement resources, and misallocated economic investment. This Article urges policymakers and partisans to stop using tropes of fear, calls for better empirical work on the probability of online harm, and proposes an Anti-Precautionary Principle — a presumption against new laws designed to stop the Superuser.

TABLE OF CONTENTS

INTRODUCTION

In 1992, a hacker accessed a computerized telephone switch in Worcester, Massachusetts.[1] He shut off phone service to the local airport and disabled the runway landing lights.[2] Over the past decade, a young Norwegian man named Jon Johansen has rankled the movie and music industries by repeatedly picking their "unbreakable" copy-protection software locks.[3] In 2001, a Russian hacker named Alexy

[1] *See infra* text accompanying notes 40-43.

[2] *See infra* text accompanying notes 40-43.

[3] *See infra* text accompanying note 36.

Ivanov broke into computer systems across America, stealing thousands of credit card numbers.[4]

These three people have done things with computers that most people could not even begin imagining how to do. They are people locked in struggles against opposing factions who regard them and the power they wield as grave threats. The Department of Homeland Security worries about the airport hacker; content owners fear the lock picker; and privacy advocates and business executives fret over the credit card number thief. A mythology has arisen around these people and countless others like them, whose stories have been repeatedly retold in the news, the halls of Congress, and the pages of law reviews.

These stories could contribute usefully to debates about important conflicts, such as computer crime, digital rights management ("DRM"),[5] and identity theft, if they were cited for what they were: interesting anecdotes that provide a window into the empirical realities of online conflict. Instead, these stories subsume the debates and substitute for a more meaningful empirical inquiry. The storytellers' pervasive attitude is, "We don't need to probe too deeply into the empirical nature of power in these conflicts because these stories tell us all we need to know." Hackers can kill airline passengers, DRM is inherently flawed, and computer criminals steal identities by the thousands. Through the spread of myth in a cluttered rhetorical landscape, these fears become not merely possible, but inevitable.

Storytelling is epidemic in debates about online disputes. The dominant rhetorical trope is the myth of power grounded in fears of the Internet. The myth infects these debates, leading policymakers to harmful, inefficient, and unwarranted responses because the myth is usually exaggerated and often untrue.

Most Internet users are unsophisticated, exercising limited power and finding themselves restricted by technological constraints, while a minority have great power and can bypass such constraints. This Article focuses on the powerful user — the Superuser. He (always he) is a mythical figure: difficult to find, expensive to catch, able to circumvent any technological constraint, and aware of every legal loophole.

[4] *See infra* text accompanying notes 75-76.

[5] Digital rights management refers to technologies used to control access to content, often copyrighted content. *See infra* Part I.B.1.

In this Article, I argue that there is too much focus on the Superuser.[6] For most online conflicts, the Superuser likely plays a very small role. To prove this general point, I focus on three of the most pressing and contested ongoing online controversies: DRM, unauthorized access to computers, and government search and surveillance of computers and networks. I revisit these important battlegrounds throughout the Article to demonstrate how Superuser rhetoric has distorted debate and driven policy, despite the absence of empirical evidence that Superusers play an important role on these battlegrounds and despite the presence of some evidence to the contrary.

Further, I argue Superuser stories spring from a widely held fear of the Internet. The link between fear and the Superuser exemplifies some general conclusions from behavioral economics and cognitive psychology about fear and how it causes people to exaggerate risk by triggering biases and heuristic shortcuts.

This Article's examination of the Myth of the Superuser extends the pre-existing literature by questioning assumptions about the role of experts. Unlike their counterparts in other fields, experts in network security and computer crime usually make the same errors in

[6] To date, no one has taken a comprehensive, theoretical, and systematic look at the harm that results from over-attention to and exaggeration of the powerful computer user. A few scholars have discussed this idea in passing. For example, Professor Lawrence Lessig has distinguished between "hackers" and "the rest of us" and has argued that the existence of the former should not stop us from trying to solve problems that primarily affect the latter. Lawrence Lessig, *Constitution and Code*, 27 CUMB. L. REV. 1, 3 (1997) ("I don't choose whether to obey the structures that [code] establishes — hackers might, but hackers are special. . . . For the rest of us, life in cyberspace is subject to the code of cyberspace, just as life in real space is subject to the code of real space"); Lawrence Lessig, *The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation*, 5 COMMLAW CONSPECTUS 181, 184 (1997); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 896 n.80 (1996) [hereinafter Lessig, *Reading*]; Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1408 n.17 (1996) (explaining that "what hackers do doesn't define what the effect of law as code is on the balance of the non-hacker public").

Professor Timothy Wu has advanced a similar theme. *See* Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1203-04 (1999) ("[E]xpert users suffer least and benefit most from an unregulated Internet. . . . [T]o stick everyone with the constitution of the expert user may, in the long run, prove the inexpert move, as it may do more to close out the Internet than flexibility ever would."); *see also* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 123 (2006) (predicting world in which minority users "with all the time and expertise" continue to download free music while rest use legitimate pay sites).

None of these scholars has explored the exaggerated Myth of the Superuser more deeply, situated these observations within the sociological literature of fear, examined the negative effects that result from relying on the Myth, or provided detailed prescriptions for dealing with these effects.

judgment as laypeople. These experts spout blusterous exaggeration about online threats rather than acting as calm, measured assessors of truth. In part, these experts have been led astray by incorrect assumptions about the malleability of code and misinterpretations of Lessig's observations about code and law.[7]

I define the Superuser and the Myth of the Superuser ("Myth") in Part I and establish that the Myth is often an exaggeration. In Part II, I show how undue attention to the Myth of the Superuser has been harmful to civil liberties, efficient and effective law enforcement, and sensible Internet regulation. In Part III, I tie the persistence of the Myth to the widely held fear of the Internet. Faced with the general public's fear, experts have abandoned their responsibility to be dispassionate truth seekers and instead have engaged in the rhetoric of myth and exaggeration.

Finally, in Part IV, I offer prescriptions for lawmakers, judges, and scholars to blunt the use and effect of the Myth. First, I challenge a set of commonly used rhetorical tools that are the hallmark of Superuser myth-telling. Second, I call for a new approach for counting Superusers. Finally, I urge regulators to adopt an Anti-Precautionary Principle — in the absence of any empirical proof about an online threat or harm, legislators should refrain from regulating anew.

In the ongoing dialogue about how best to regulate virtual, constructed spaces, we find ourselves awash in metaphor, analogy, and myth. These myths carry great weight, repeated by those with the trappings of authority and never challenged for accuracy or even plausibility. By calling into question the dominant myth, the Myth of the Superuser, I try to restore some of what we have lost: constructive debate and carefully reasoned regulation.

I. THE SUPERUSER AND THE MYTH

The rhetorical devices I define in this Part are not uncommon; they are pervasive. Every important debate about online conflict leads eventually to one or both sides making claims about the Superuser.[8]

[7] *See generally* LAWRENCE LESSIG, CODE: VERSION 2.0 (2d ed. 2006) (describing how code regulates online behavior).

[8] I restate it as a less-charged version of Godwin's Law: As a debate about online conflict grows longer, the probability of an argument involving powerful computer users approaches one. MIKE GODWIN, CYBER RIGHTS 48 (1998) ("As an online discussion grows longer, the probability of a comparison involving Nazis or Hitler approaches one."). I would call it "Ohm's Law," but that is already taken.

A. The Superuser and the Myth Defined

1. The Superuser

A few terms must be defined. As used in this Article, "power" is the ability to control or change computers or networks. If computer users are rank-ordered by the amount of power they possess, the "ordinary user" is, roughly speaking, the user in the middle.

A "Superuser" is a computer user who possesses power that the ordinary user does not.[9] He can control or change computers and networks in extraordinary ways. Superusers tend to have more time, practice, knowledge, or access to tools than ordinary users.[10] Tools play a particularly important and complex role. Superusers often use sophisticated computer programs (sometimes created by them, often created by others) to gain power.[11]

[9] A note on terminology: the word "Superuser" has not been used before in legal scholarship with precisely this meaning. In various versions of UNIX and UNIX-like Operating Systems, "superuser" (lowercase "s") is the name given to the user account that a system administrator can use to make almost any change to the system. *See* EVI NEMETH ET AL., UNIX SYSTEM ADMINISTRATION HANDBOOK 39 (3d ed. 2001). This is also known as the "root" account. *Id.* at 37. Some commentators have used this meaning of superuser. *See, e.g.*, Richard W. Downing, *Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime*, 43 COLUM. J. TRANSNAT'L L. 705, 721 (2005) (discussing hacker who "gains 'root level' access, also known as 'superuser' status").

My meaning is different, and in this Article I capitalize "Superuser" to distinguish it from the prior, UNIX definition. Several technically minded readers have criticized my decision to give a new meaning to this word, accusing me of muddying an otherwise clear term or, less charitably, suggesting that it betrays a lack of technical knowledge or acumen. See the various comments to Slashdot, http://it.slashdot.org/article.pl?sid=07/04/11/1952247 (last visited Apr. 3, 2008) and The Volokh Conspiracy, http://www.volokh.com/posts/1176127892.shtml (last visited Apr. 3, 2008).

I decided to use the term Superuser despite these criticisms because it concisely captures the idea of "power without necessary malice" that alternatives like "hacker" or the neologism, "superhacker" do not convey. Also, although many computer experts — particularly UNIX specialists — know the term's other meaning, most noncomputer specialists, including policymakers, do not. Finally, even for those who know the earlier, UNIX meaning of the term, it should be easy to understand which of the two meanings is meant from context.

[10] *Cf.* Paul Graham, *Great Hackers*, July 2004, http://www.paulgraham.com/gh.html (describing skills required to be hacker); Eric Steven Raymond, *How to Become a Hacker*, http://catb.org/~esr/faqs/hacker-howto.html (last updated Jan. 8, 2008) (same). Often, they have more than one of these, but they need not have all of them.

[11] CHRIS PROSISE & KEVIN MANDIA, INCIDENT RESPONSE & COMPUTER FORENSICS 385-414 (2d ed. 2003) (entitling chapter "Investigating Hacker Tools"); Graham, *supra*

But once a tool becomes widely used, its users are considered ordinary users and not Superusers. For example, in the late 1990s, Napster users could browse and copy the music collections of millions of others, yet they were not Superusers.[12] Because many people used their software, these people were merely empowered ordinary users. In other words, the term Superuser is a relative one. Having power — the ability to effect change — is necessary but not sufficient to be a Superuser.

The term can come and go with time. A person with power X is a Superuser only as long as the percentage of people with X is small. Usually, that percentage increases over time, and once X becomes accessible to many people, the Superuser designation disappears.

Consider audio compact disc ripping. Not long ago, when CDs and the computer drives that could read them were both new and scarce, few people (all Superusers) could copy the music from a CD onto a computer or "rip" the CD.[13] It was not long, however, before Superusers packaged this power into functional but unpolished computer programs used by people not considered Superusers.[14] Today, the ability to rip a CD is no longer a Superuser power. This is the result of programmers making ripping programs both easier to obtain[15] and use.[16]

note 10 ("Like all craftsmen, hackers like good tools.").

[12] *See* A&M Records v. Napster, Inc., 239 F.3d 1004, 1010-13 (9th Cir. 2001) (describing Napster).

[13] *See* Mike Snider, *Microsoft, Macrovision Join to Halt CD 'Ripping,'* USA TODAY, Apr. 24, 2003, at 5D.

[14] When Superusers package their power into tools, the empowered but ignorant users are often called script kiddies. *See* SIMSON GARFINKEL, WEB SECURITY, PRIVACY AND COMMERCE 401 (2d ed. 2002). We will consider the script kiddie again in Part IV.D.2.

[15] CD ripping software now comes bundled, for example, with Windows XP/Windows Media Player and Mac OS X/iTunes. *See* Apple Inc., *iTunes 7: How to Improve Performance While Burning or Ripping CDs*, http://docs.info.apple.com/article.html?artnum=304410 (last visited Apr. 3, 2008); Windows Media, *Ripping CDs in Windows Media Player*, http://www.microsoft.com/windows/windowsmedia/knowledgecenter/mediaadvice/0080.mspx (last visited Apr. 3, 2008).

[16] There are countless other examples of the passage of time redefining Superuser power. Consider photo sharing. A decade ago, to share photos on the web, you had to scan physical prints into digital files, upload the files using the file transfer protocol, write (without the assistance of any specialized tools) a web page containing those photos, and then email the URL to your friends and relatives. A little less than a decade ago, you could use an early-model digital camera and a web-hosting service like Geocities to develop a photo gallery using better but still clunky tools. Today, an account with Flickr or Kodak Gallery accomplishes the same goal in much less time with significantly better results.

Further, to send an anonymous email in the early 1990s, you had to issue a series of

Not all Superusers act with malice or try to cause harm. There are good Superusers, bad Superusers, and morally neutral Superusers. As the CD ripping example demonstrates, sometimes the morality of a Superuser's power is in the eye of the beholder. Most people consider CD ripping a morally neutral act, but some copyright owners may see it as a harmful, negative act.[17]

2. The Myth of the Superuser

The "Myth of the Superuser" is the belief that an online conflict cannot be resolved without finding a way to neutralize Superusers. As I explore more fully in Part I.D, the Myth is flawed. Superusers are often inconsequential because they are uncommon or unable to cause great change. Thus, I argue solutions targeted at ordinary users are good enough.

The Myth also refers to any argument that invokes the Superuser to support or oppose a proposed solution to an online conflict. Consider Congress's rhetoric supporting amendments to the Computer Fraud and Abuse Act ("CFAA"), the federal law criminalizing computer hacking and trespass, codified in § 1030 of title 18 of the U.S. Code.[18] Specifically, consider the 1996 Senate Committee Report[19] ("1996

precise commands (which complied with the SMTP email protocol) to an email server. In the late 1990s, anonymous remailers in foreign countries would strip identifying information from incoming messages and forward them onto their destination. Today, setting up an account at Yahoo! Mail or Gmail quickly enables one to send pseudonymous email messages.

[17] *See* Posting of Fred von Lohmann to Deeplinks Blog, http://www.eff.org/deeplinks/archives/004409.php (Feb. 15, 2006) (quoting RIAA in regulatory filing as saying, "creating a back-up copy of a music CD is not a non-infringing use").

[18] Congress adopted § 1030 in 1984. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, tit. II, Pub. L. No. 98-473, § 2101, 98 Stat. 1837, 2190. It has made at least five major revisions to § 1030 since then. *See, e.g.*, Homeland Security Act of 2002, tit. II, Pub. L. No. 107-296, sec. 225, § 1030, 116 Stat. 2135; Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, tit. V, Pub. L. No. 107-56, sec. 506, § 1030, 115 Stat. 272, 278; Economic Espionage Act (EEA) of 1996, Pub. L. No. 104-294, 110 Stat. 3488, 3491-95; Violent Crime Control and Law Enforcement Act of 1994, tit. XXIX, Pub. L. No. 103-322, sec. 290001, § 1030, 108 Stat. 1796; Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, sec. 2, § 1030, 100 Stat. 1213. These frequent amendments are surprising, given the infrequency with which the law is used. *Cf.* Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 823-24 (2003) (noting relative infrequency with which computer privacy provisions of 18 U.S.C. § 2701 are invoked).

[19] *See generally* S. REP. NO. 104-357 (1996).

Report") accompanying broad amendments to the CFAA.[20] This report is a model of Superuser storytelling, full of questionable rhetorical devices typical of the Myth.[21]

First, Superuser stories are simultaneously detailed and vague. They richly describe events but omit the names, dates, and places needed to corroborate the story.[22] The 1996 Report is full of anecdotes about nefarious Superusers. For example, the Committee asserted that "[h]ackers . . . have broken into . . . supercomputers for the purpose of running password cracking programs."[23] The hackers and victims are anonymous, and the authors never say whether these mythical criminals were caught or whether gaps in the law hindered attempts to prosecute them.

Second, Superuser storytellers summarize trends using vague adverbs like "often," "usually," and "frequently."[24] To justify broadening the scope of a crime under the CFAA, the Committee asserted that "intruders *often* alter existing log-on programs so that

[20] National Information Infrastructure Protection Act (NIIPA) of 1996, tit. II, Pub. L. 104-294, § 201, 110 Stat. 3488, 3491-94 (passing NIIPA as Title II of EEA).

[21] The Economic Espionage Act ("EEA"), which criminalizes certain trade secrets thefts (codified at 18 U.S.C. §§ 1831-1839 (2000 & Supp. V 2005)), is another example of a computer crime law whose prosecution record does not seem to match the hype and rhetoric used by those who urged the creation of the law. *See* Joseph F. Savage, Jr., Matthew A. Martel, & Marc J. Zwillinger, *Trade Secrets Conflicting Views of the Economic Espionage Act*, 15 CRIM. JUST. 10, 11-12 (2000) (contrasting foreign government prohibitions of Act with domestic trade secret theft provision that has been frequently used). Consider the views of two defense attorneys (writing with a former federal prosecutor) about the EEA:

> The congressional debates contained dire accounts of foreign governments pilfering America's trade secrets. Simply put, the EEA was couched in terms of national security. . . . Because of this original focus, one might surmise that the DOJ would immediately give priority to enforcement procedures involving foreign spies. Instead, not one prosecution has occurred enforcing the foreign espionage provisions of the EEA. Not a single one. The conclusion seems inescapable: The foreign economic espionage law either was not necessary or there is a real and ongoing problem that is not being addressed.

Id. at 11.

[22] *Cf.* Michael Levi, *"Between the Risk and the Reality Falls the Shadow": Evidence and Urban Legends in Computer Fraud (with Apologies to T.S. Eliot)*, *in* CRIME AND THE INTERNET 44, 46 (David S. Wall ed., 2001) (discussing computer security experts' claims that events happened, but discussing those claims without pertinent details in service of client confidentiality).

[23] S. REP. NO. 104-357, at 9.

[24] *See, e.g.*, *id.* at 11.

user passwords are copied to a file that the hackers can retrieve later."[25] Again, the Committee provided no other details.

Third, Superuser storytellers pass the buck, parroting back what others have told them. To justify a new crime to address the allegedly pressing problem of people making threats against computer systems,[26] the Committee said, "According to the Department of Justice [("DOJ")], threats have been made against computer systems in several instances."[27] The DOJ's authorship of the vague claim is the only proof of its relevance and veracity.

Fourth, Superuser stories are often hypothetical. To justify the same computer threat provision, the Committee mused, "One can imagine situations in which hackers penetrate a system, encrypt a database and then demand money for the decoding key."[28]

These are not the only strategies employed by Superuser storytellers. They also rely on exaggeration, jargon, strained metaphors, appeals to common sense and common knowledge, and other rhetorical sleights-of-hand.[29]

B. The Superuser and Online Conflict

In every online conflict, partisans wield the Myth of the Superuser like a rhetorical bludgeon.[30] The Superuser has become a form of what sociologist Stanley Cohen termed the "folk devil":[31] members of

[25] *Id.* (emphasis added).

[26] *See* 18 U.S.C. § 1030(a)(7) (2000) (making it crime to, "with intent [] extort from any person any money or other thing of value, transmit[] in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer").

[27] S. REP. NO. 104-357, at 12.

[28] *Id.*

[29] *See* PAUL A. TAYLOR, HACKERS: CRIME IN THE DIGITAL SUBLIME, at xii (1999) ("The rhetoric of the digital sublime describes the particularly high levels of hyperbole that seem to surround computer-based technologies.") (emphasis omitted); MAJID YAR, CYBERCRIME AND SOCIETY 24-25 (2006) (describing "hyperbole" of "official pronouncements on hacking").

[30] The phrase "online conflict" is purposefully broad and used to describe any of the disputes, lawsuits, or debates that have arisen as a result of the emergence of the Internet. In the pages that follow, the necessarily vague term is used somewhat inconsistently, on occasion to describe very specific clashes between well-defined stakeholders, while on others to describe more amorphous disagreements between less clearly delineated sides.

[31] STANLEY COHEN, FOLK DEVILS AND MORAL PANICS: THE CREATION OF THE MODS AND ROCKERS 9-11 (1972); *cf.* Carol Sanger, *Infant Safe Haven Laws: Legislating in the Culture of Life*, 106 COLUM. L. REV. 753, 782 (2006) (discussing Cohen's theories of folk devils and moral panics in context of infanticide).

society seen as dangerous or deviant, blamed for many of society's ills.[32] The trope arises in every single branch of Internet law, including intellectual property, computer crime, information privacy, information security, Internet governance, telecommunications, innovation policy, First Amendment law, and jurisdiction.

This Article focuses on three important conflicts: DRM, computer crime, and computer search and seizure. These represent a broad cross- section of policy concerns and styles of debate and argument. These also raise three different sets of institutional concerns, because these debates have been targeted, primarily and respectively, at scholars, legislators, and judges.

1. Music and Movie Piracy and DRM

DRM systems allow content owners to control what other people can do with data.[33] A fierce debate over DRM rages, focusing largely on whether DRM systems should stand or fall on their own technical merits, or if instead they should be bolstered by laws that make it illegal to circumvent DRM (i.e., pick the locks) or to teach others to do the same.[34] The Superuser looms large in the debate because he can pick locks that ordinary users cannot.

Consider again Jon Johansen. Apple's iTunes Music Store sells songs protected by a DRM technology called FairPlay, which lets purchasers listen to the music they have bought only in authorized ways and only on authorized computers.[35] Johansen, a Superuser *par excellence*, has repeatedly created programs that can strip the

[32] *See* John Timmer, *Breaches of Personal Data: Blaming the Myth and Punishing the Victim*, ARS TECHNICA, Mar. 14, 2007, http://arstechnica.com/news.ars/post/20070314-breaches-of-data-blaming-the-myth.html (explaining that "hackers have become the folk devils of computer security").

[33] *See generally* Dan Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537 (2005) (discussing role DRM plays in shaping and replacing technical and legal standards); Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003) (identifying connection between DRM and privacy protection); Randall Picker, *Mistrust-Based Digital Rights Management*, 5 J. ON TELECOMM. & HIGH TECH. L. 47 (2006) (proposing methods for disincentivizing DRM circumvention by tying copies of works to purchaser).

[34] *See* Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161, 162-63 (1997); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need To Be Revised*, 14 BERKELEY TECH. L.J. 519, 522-23 (1999).

[35] Steve Jobs, CEO of Apple, has publicly called the use of DRM for music into question. Steve Jobs, CEO, Apple Inc., *Thoughts on Music* (Feb. 6, 2007), http://www.apple.com/hotnews/thoughtsonmusic/.

protection from a FairPlay-protected song, empowering users to access iTunes-purchased music in ways that Apple has tried to forbid.[36]

2. Computer Security and Unauthorized Access

Computer security systems protect Internet-connected computers from unauthorized intruders.[37] These security systems are complex.[38] Because of this complexity, software tends to be riddled with vulnerabilities, many of which can be exploited by Superusers to gain unauthorized access.[39]

For example, in the early 1990s, a young man bypassed a computer's security system to gain access to a computer in Worcester, Massachusetts that controlled an important telephone switch.[40] Inadvertently, he reset the switch, disabling local phone service to the area, which included a small, unmanned airport.[41] By disabling the switch, he made it impossible for incoming aircraft to turn on the landing lights.[42] No planes crashed, and nobody was injured. But advocates to this day retell the story to policymakers, spinning terrifying variations: replace the juvenile with international terrorists, the small regional airport with O'Hare International Airport, and the

[36] *See* Robert Levine, *Unlocking the iPod*, FORTUNE, Oct. 30, 2006, at 73.

[37] *See generally* Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J.L. & PUB. POL'Y 283, 285 (2006) (giving "a comprehensive assessment of the software security issue using a law and economics framework").

[38] *Id.* at 319 (discussing market pressures that lead security software to include many features, increasing complexity of security systems).

[39] *Id.* at 296 ("Given the complexity of programs such as these, most experts believe that bugs and other vulnerabilities are inevitable.").

[40] Many public and private figures have retold this story, perhaps most prominently Scott Charney in a report issued by the House of Representatives. *See* Scott Charney, *Transition Between Law Enforcement and National Defense*, *in* SECURITY IN THE INFORMATION AGE: NEW CHALLENGES, NEW STRATEGIES 52 (Robert F. Bennet ed., 2002), *available at* http://www.house.gov/jec/security.pdf. At the time he authored this report, Charney was a principal at PricewaterhouseCoopers. Immediately before he took that position, however, he had been a long-standing career employee at the DOJ, where he founded and served as Chief to the Department's Computer Crime and Intellectual Property Section. After leaving PricewaterhouseCoopers, he became Microsoft's Vice President for Trustworthy Computing. *See* Microsoft Corp., http://www.microsoft.com/presspass/exec/charney/default.mspx (last visited Apr. 3, 2008) (providing Scott Charney's biography).

[41] *See* Charney, *supra* note 40, at 54.

[42] *See id.* at 54-55.

inadvertent effect with an intentional attack, and the lesson is unmistakable.[43]

3. Surveillance

The War on Terror has given birth to many stories, including the tale of the cat-and-mouse game between competing groups of Superusers: terrorist data hiders and government data finders.[44] Government agents use complex tools and techniques to sift through large volumes of data stored on computers and coursing through networks.[45] They would usually find the evidence they sought, we are told, if not for Superuser data hiders and their creative and evolving techniques.[46]

Versions of the following myth are told often in law enforcement circles.[47] FBI agents serve a warrant to search John Smith's house and seize any computers found. Amid the usual chaos of an ongoing search, an agent notices that a computer in the corner is whirring loudly. Later, a forensic analysis reveals that a large portion of the computer's hard drive has been wiped clean, supporting fears that Smith had triggered a software "logic bomb" after learning of the search. It is a compelling story, but I could find no documented examples suggesting that the myth had any basis in reality.

C. *The Myth of the Superuser in the Noncomputer World*

Are Superusers limited to the virtual world? Are there not people in the physical, nonvirtual world with the knowledge, time, training, or resources to flout technical and legal constraints? Consider locks. Very few people know how to pick them. For most of us, locks keep

[43] *See id.* at 55 (comparing Worcester incident to potential attack on O'Hare International Airport).

[44] *See infra* Part II.B.

[45] Orin Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 538 (2005).

[46] *See id.* at 546-47.

[47] Books about computer forensics, for example, often describe the supposedly widespread use of "logic bombs" or "kill switches." *See* JOHN W. RITTINGHOUSE & WILLIAM M. HANCOCK, CYBERSECURITY OPERATIONS HANDBOOK 390 (2003) ("Since most good computer criminals are trying to avoid detection and prosecution, they will often employ the use of logic bombs embedded within system administrative processes commonly required during investigations."); JOHN R. VACCA, COMPUTER FORENSICS: COMPUTER CRIME SCENE INVESTIGATION 238 (2d ed. 2005) ("The computer investigator . . . needs to be worried about destructive process and devices being planted by the computer owner . . . .").

us out of places we are not meant to go and secure things that we might otherwise want to take.

In the physical world, lawmakers often exaggerate the criminal threat to justify broad criminal prohibitions and new law enforcement surveillance capabilities. Witness the rhetoric surrounding child abductions or school shootings. These crimes are often said to be epidemic despite numerous studies that conclude otherwise.[48] If Superusers and the Myth thrive offline as well as online, what is gained by focusing solely online? Is there anything special about this context?

Despite some similarities between the online and offline uses and abuses of power, there are many differences between the two. These differences make the online threat of the Myth of the Superuser much more prevalent and vexing. The Myth of the Superuser is different in kind and degree from real world analogs. The most important difference is the type of power. The online Superuser is said to possess science fiction-like abilities unlike the much more constrained power attributed to his physical world counterparts.[49] Fear of unbounded power leads policymakers to regulate online harms in much more broad, vague, sweeping, and as I argue later, harmful ways.[50]

In the real world, the Myth of the Superuser is invoked less often because countervailing voices oppose exaggerated threats, soothing fears and debunking myths.[51] Academic researchers and some in the media, for example, use statistics to show that concerns about

[48] *See* Diana Griego & Louis Kilzer, *The Truth About Missing Children: Exaggerated Statistics Stir National Paranoia*, DENVER POST, May 12, 1985, at 1-A (debunking, in Pulitzer Prize winning series, exaggerated fears about child abductions); Lynnell Hancock, *The School Shootings: Why Context Counts*, COLUM. JOURNALISM REV., May-June 2001, at 76 (concluding statistics support view that public's increased fear of school shootings was "exaggerated, fed by saturation media coverage that is painting a distorted picture").

[49] *See infra* Part III.B.2 (describing nature of Superuser's power).

[50] *See infra* Part II. The closest real world parallel is the "Superterrorist," an increasingly mythologized figure whose command over the physical world approaches the Superuser's control of the online world. The Superterrorist is a master at evasion, able to plan and fund complex crimes without leaving behind any tracks. Because too much can be made of this comparison, I spend very little additional space developing it. I believe, however, that some of the observations and prescriptions that follow apply to the terrorism context, as well. There is one especially salient connection between terrorism and computer crime. Many have taken to talking about the "cyberterrorist," who allegedly advances terror goals by attacking computer systems. *See* Joshua Green, *The Myth of Cyberterrorism*, WASH. MONTHLY, Nov. 2002, http://www.washingtonmonthly.com/features/2001/0211.green.html (debunking claims of prevalence of cyberterrorism).

[51] *See, e.g.*, sources cited *supra* note 48.

particular types of harmful behavior are overblown.[52] For reasons that I will discuss in depth, this rarely happens with online risks.[53]

Finally, although lawmakers sometimes fall prey to the Myth in regulating physical space, they often do not. Consider locks again. Criminal laws prohibiting theft and breaking and entering are still considered effective despite the fact that some people can pick locks.[54]

D. Dispelling the Myth of the Superuser

British criminologist David S. Wall has remarked:

> Fears, which, in the absence of reliable information to the contrary, have been nurtured and sustained by media sensationalism. Yet, our practical experience of the Internet is that few of these fears have actually been reali[z]ed. Furthermore, there is clearly emerging a body of evidence to show that the criminal reality of the Internet is not the all engulfing 'cyber-tsunami', but, like the terrestrial world, a large range of frequently occurring small-impact crimes.[55]

Superusers may walk among us, but they usually do so in small enough numbers to be safely ignored. Even though a few Superusers can cause harm, they are so difficult to find and apprehend, so resistant to ordinary disincentives, or constitute so small a part of the problem that they are not worth the hunt. Of course, even a few Superusers demand attention if they are powerful enough to account for a significant portion of the harm. Measuring the impact of the Superuser requires more than a head count; it must also account for the amount of harm caused by any one Superuser. Three reasons illustrate why the Myth is an exaggeration.

[52] *See infra* Part I.D.1.

[53] *See infra* Part III.

[54] *See* Lessig, *Reading*, *supra* note 6, at 896 n.80 (explaining that "from the fact that 'hackers could break any security system,' it no more follows that security systems are irrelevant than it follows from the fact that 'a locksmith can pick any lock' that locks are irrelevant"); Wu, *supra* note 6, at 1195 (asking people to "[c]onsider for a moment the observation that a lock may be picked; interesting, no doubt, but not a convincing demonstration that a lock cannot serve any regulating function").

[55] *See* CRIME AND THE INTERNET, *supra* note 22, at xi.

1. Myth-Dispelling Studies and Statistics

Statistics suggest the Superuser is a myth.[56] In 2006, two researchers at the University of Washington surveyed twenty-six years of national print and broadcast news for stories about electronic data loss.[57] In all, 550 separate incidents were studied, amounting to the reported loss of 1.9 billion records, or nine private records for every adult living in the United States.[58] The researchers tested the conventional wisdom that hackers were mostly to blame for the loss of personal data.[59] To the contrary, "for the period between 2000 and 2006, 31% of the incidents were about a breach caused by a hacker, 8% of the incidents involved an unspecified breach, and 61% of the incidents involved different kinds of organizational culpability."[60] Organizational culpability included cases involving accidental records release, employee misconduct, misplaced backup tapes, and stolen laptops.[61]

As another example, British sociologist Michael Levi focused on studies of victimization rates for computer crime. He concluded that they showed much less victimization than contemporary media accounts had suggested.[62] Granted, many of these studies are by now a decade old or older. But at least when Levi drew his conclusions, the numbers did not seem to square with the public rhetoric.

Levi noted "international surveys in 1996 and 1998 [by Ernst & Young] . . . turned up very few cases of reported or unreported computer frauds."[63] He also cited these older studies to show that although more than two-thirds of executives in large private sector

[56] Part IV discusses better available and more reliable sources for statistics.

[57] Kris Erickson & Philip N. Howard, *A Case of Mistaken Identity? News Accounts of Hacker and Organizational Responsibility for Compromised Digital Records, 1980-2006*, 12 J. COMPUTER MEDIATED COMM. 1, 3 (2007). The studies included all stories from 1980 to 2006, using both the LexisNexis and Proquest databases.

[58] *Id.* at 12-13.

[59] *Id.* at 3 (stating that "the campaign against hackers has successfully cast them as the primary culprits to blame for insecurity in cyberspace").

[60] *Id.* at 17. Even if the entire 8% of the unattributed breaches were the result of hackers, hackers would still account for only 39% of the reported incidents.

[61] *Id.* at 17-18. Erickson and Howard note, however, that hackers accounted for a vast majority of the number of stolen records, but only because one incident — data theft from the Acxiom Corporation that led to a criminal conviction — involved the loss of 1.6 billion records. *Id.* at 18. If that single incident is removed from the data set, hackers caused 32% of lost data, organizational behavior caused 48%, and 20% remains unattributed. *Id.*

[62] Levi, *supra* note 22, at 51-55.

[63] *Id.* at 53 (citing 1996 and 1998 studies by Ernst & Young).

companies felt computer viruses and hacking were serious concerns, only 11% had experienced either and only 5% had experienced both.[64] A U.K. government-run audit similarly found that the number of entities reporting information technology fraud fell from 10% in 1994 to 8% in 1997.[65]

Further, statistics suggesting that the Superuser is a potent force are often rebuttable. The statistics most cited about computer security incidents are those reported in the annual Computer Security Institute ("CSI") / FBI Computer Crime and Security Survey ("Survey"), a new version of which has been released every year for over a decade.[66] The Survey may be the media's pre-eminent source for statistics about online harm.[67] When they cite the Survey, the media often report the results in breathless tones.[68] Dozens of law review articles and student notes have also cited the Survey.[69]

[64] *Id.*

[65] *Id.* at 51-52 (citing results from three reports by Audit Commission). Levi noted that despite this drop, the average cost to each victim rose and the percentage of respondents reporting other "IT abuse" rose during the same period. *Id.*

[66] LAWRENCE A. GORDON ET AL., 2006 COMPUTER SECURITY INSTITUTE / FBI COMPUTER CRIME AND SECURITY SURVEY, *available at* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

[67] Ira Winkler, Opinion, *Investigating the FBI's 'Invalid' Security Survey*, SEARCHSECURITY.COM, Jan. 19, 2006, http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1159992,00.html (stating that Survey is "often referred to as 'the most quoted stud[y] in the field'").

[68] The release of the 2006 Survey prompted this reporting: "Virus attacks, unauthorized access to computer systems and other forms of cybercrime account for up to 75% of the financial losses at U.S. companies." Tim Scannell, *Computer Crime and the Bottom Line*, INTERNETNEWS.COM, July 20, 2006, http://www.internetnews.com/stats/article.php/3621236.

[69] A search of the Westlaw JLR database on January 24, 2008, for the string "CSI" /S "COMPUTER CRIME" /S "SURVEY" returned 57 hits. *See, e.g.*, Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23, 31-32 (2006) (citing Survey's reported incidence of Denial of Service attacks); Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455, 521 (2006) (citing Survey's finding that 70% of computer intrusions are traceable to Internet connection); Bruce P. Smith, *Hacking, Poaching, and Counterattacking: Digital Counterstrikes and the Contours of Self-Help*, 1 J.L. ECON. & POL'Y 171, 171 n.1 (2005) (citing Survey's statistics about spread of antivirus and firewall software); Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 201 n.5 (2006) (citing Survey's report of $130 million damages from unauthorized use of computers).

The Survey's methodology, however, is entirely suspect.[70] First, the Survey is sent only to members of the CSI.[71] Second, in 2006, the Survey was returned by a mere 12% of those who had received it.[72] Although past editions of the Survey bore a disclaimer that the results were not statistically significant, recent versions do not contain the same disclaimer.[73] Although these methodological shortcomings do not point toward a systematic inflation or deflation of results, they do call into question the authority with which the Survey is usually regarded and cited. Further, even if the Survey results are given any credence, they show that both the level of computer security incidents and money spent on response have been decreasing steadily for the past four years.[74]

2. Myth-Dispelling Anecdotes

The second reason to doubt claims about Superuser power is that anecdotally, some online crimes seem to be committed by ordinary users much more often than by Superusers. Consider the growing problems of data breach and identity theft. Data breachers are often portrayed as genius hackers who break into computers to steal thousands of credit cards.[75] Although there are criminals who fit this profile, the police increasingly focus on people who obtain personal data in much more mundane, non-Superuser ways.[76] For example,

[70] *See* Winkler, *supra* note 67 (criticizing 2005 Survey), Bill Brenner, *Security Blog Log: Has CSI/FBI Survey Jumped the Shark?*, SEARCHSECURITY.COM, July 21, 2006, http://searchsecurity.techtarget.com/columnItem/0,294698,sid14_gci1202328,00.html; Posting of Chris Walsh to Emergent Chaos, http://www.emergentchaos.com/archives/2006/07/csifbi_survey_considered.html (July 16, 2006, 01:28) (challenging methodology behind Survey).

[71] *See* GORDON ET AL., *supra* note 66, at 1, 26 (listing Survey's methodology); *see also* Winkler, *supra* note 67 (suggesting that sample is not representative). For example, the demographics have shifted in the 11 years of the survey. *Id.* In the 2005 Survey, the percentage of respondents who belong to the information sharing group INFRAGARD and the percentage who use Intrusion detection system (IDS) software differ widely from the results of an earlier version. *Id.*

[72] *See* GORDON ET AL., *supra* note 66, at 19.

[73] *See* Winkler, *supra* note 67.

[74] *Id.*

[75] *See* Tom Zeller, Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. TIMES, Feb. 24, 2005, at C1 (quoting Senator Dianne Feinstein: "Existing laws . . . are no longer sufficient when thieves can steal data not just from a few victims at a time, but from thousands of people with vast, digitized efficiency.").

[76] *See, e.g.*, Press Release, U.S. Dep't of Justice, Russian Hacker Sentenced to Four Years in Prison for Supervising Criminal Enterprise Dedicated to Computer Hacking, Fraud and Extortion and Victimizing Glen Rock Financial Services Company (July 25,

laptop theft is a common, low-tech way many criminals gather personally identifiable information.[77] Recently, ChoicePoint, a data broker that has dealt with many data breach cases, concluded that "it had focused so intently on preventing hackers from gaining access to its computers through digital back doors that it had simply overlooked real-world con artists strolling unnoticed through the front door."[78]

Several studies have shown a recent decline in identity theft.[79] District attorneys in the western United States have reported that a majority of their identity theft arrestees are methamphetamine addicts.[80] Although some of these methamphetamine cases involve the use of the Internet to facilitate identity theft,[81] they also include non-Superuser techniques like trash rifling, mail theft, or check washing.[82]

Another reason to doubt claims about the scope of online identity theft is that many confuse mere data loss with identity theft.[83] As one journalist noted, "[W]hile high-profile data breaches are common,

2003), http://www.usdoj.gov/criminal/cybercrime/ivanovSent_NJ.htm (describing hacker who broke into system and stole text file containing 3500 credit card numbers).

[77] *See* Erickson & Howard, *supra* note 57, at 2 (stating that "the growing number of news stories about compromised personal records reveals a wide range of organizational mismanagement and internal security breaches: lost hard drives and backup tapes, employee theft, and other kinds of administrative errors"); Steve Lohr, *Surging Losses, But Few Victims*, N.Y. TIMES, Sept. 27, 2006, at G1; David Stout, *'Garden Variety Burglary' Suspected in Loss of Data*, N.Y. TIMES, June 9, 2006, at A24 (describing theft of laptop containing information about 26.5 million military people).

[78] Gary Rivlin, *Keeping Your Enemies Close*, N.Y. TIMES, Nov. 12, 2006, at 31 (finding that "in 2005 alone, more than forty phony businesses . . . had opened accounts that gave them unfettered, round-the-clock access to the vital data ChoicePoint maintains"); *see also id.* (summarizing conclusions of FTC report that "criminal interlopers" who stole identities from ChoicePoint were "sloppy and amateurish").

[79] *See, e.g.*, John Leland, *Identity Fraud Has Dropped Since 2003, Survey Shows*, N.Y. TIMES, Feb. 6, 2007, at A17 (reporting drop from 4.7% to 3.7% of Americans reporting being victims of ID fraud in survey sponsored by banking industry).

[80] *See* John Leland, *Meth Users, Attuned to Detail, Add Another Habit: ID Theft*, N.Y. TIMES, July 11, 2006, at A1 (reporting 60 to 70% of identity theft cases in Denver and 100% in Spokane County, Washington are tied to methamphetamine users or dealers).

[81] There are non-Superuser ways to use the Internet to assist identity theft. *See* Robert Lemos, *Google Queries Provide Stolen Credit Cards*, CNET NEWS.COM, Aug. 19, 2004, http://news.com.com/2102-1029_3-5295661.html (describing technique demonstrated at annual "Black Hat" conference for obtaining credit card numbers using public Google searches).

[82] *See* Leland, *supra* note 80. There is another way to interpret these anecdotes. District attorneys may prosecute meth-addicted identity thieves more often because they are easier to catch than the Superuser identity thieves. *See id.*

[83] *See* Lohr, *supra* note 77.

there is no evidence of a surge in identity theft or financial fraud as a result. In fact, there is scant evidence that identity theft and financial fraud have increased at all."[84]

Finally, consider briefly claims that terrorists are plotting to use computer networks to threaten lives or economic well-being. There has never been a death reported from an attack on a computer network or system.[85] In fact, despite claims to the contrary,[86] many doubt that an attack will ever successfully disable a significant part of the Internet.[87]

Admittedly, too much reliance on anecdotes may smack of hypocrisy. There is a risk of engaging in the "Myth of the Myth of the Superuser." There are limits to using opinions and qualitative evidence to disprove the Myth because they share so much in common with the anecdotes that fuel it. For this reason, I place greater stock in the statistical observations made in the prior section and in Part IV.

3. Obvious Overstatements of the Risk

Finally, some statements of the risk from Superusers are so exaggerated that they are self-disproving. For example, Richard Clarke, former Special Advisor to the President on Cybersecurity under the Clinton and second Bush Administrations, often stated that "digital Pearl Harbors are happening every day."[88] Even though the phrase "digital Pearl Harbor" can refer to many different things — attacks with the psychologically damaging effect, horrific loss of life, terrifying surprise, size of invading force, or financial toll of the

[84] *Id.*

[85] *See* Brian Krebs, *Feds Falling Short on Cybersecurity; Former Cybersecurity Adviser Urges More Resources to Battle Cyberterror*, WASHINGTONPOST.COM, Apr. 8, 2003, http://seclists.org/isn/2003/Apr/0036.html (quoting Richard Clarke testifying in House Government Reform subcommittee: "For many, the cyber threat is hard to understand; no one has died in a cyberattack, after all, there has never been a smoking ruin for cameras to see.").

[86] *See* NAT. INFRASTRUCTURE ADVISORY COUNCIL, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 6 (2002), *available at* http://www.whitehouse.gov/pcipb/ [hereinafter NATIONAL STRATEGY].

[87] *Frontline: Cyber War!* (PBS television broadcast) (Mar. 20, 2003) (interview of Scott Charney), *available at* http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/charney.html. "[I]t's not as easy to take down the Internet as some might believe. There's a lot of redundancy, a lot of resiliency in the system. . . . I still think today the concern of a broad, sweeping global Internet attack that had long enough staying power is not our number one threat today." *Id.*

[88] *See* Scott Berinato, *The Future of Security*, COMPUTERWORLD, Dec. 30, 2003, *available at* http://www.computerworld.com/newsletter/0,4902,88646,00.html.

December 7, 1941 event — the claim is a horribly exaggerated overstatement regardless of Clarke's intended meaning.[89]

4. The Scope of the Claim

These statistics and anecdotes suggest that many stories about Superusers are exaggerated. Due to the incomplete nature of the empirical evidence, this Article does not claim that the Superuser is always a myth. Doubtless, some online harms are committed solely by Superusers, and some Superusers probably cause significant harms. Nevertheless, this survey of the empirical evidence should cast great suspicion on the conventional account of unbridled power. And, as I will demonstrate in the next Part, this empirical evidence should give policymakers significant pause in light of the harms that flow from attempting to regulate the Superuser.

II. Harms of the Myth

Why should we care whether exaggerated arguments about Superusers cause legislators to address risks that are unlikely to materialize? Aside from dead-letter statutory prohibitions, are there any other harms that flow from the Myth of the Superuser? The answer is yes, there are significant harms. Moreover, the near-universal belief in the Myth means there has never been an accounting of these harms, and thus we are doomed to repeat and extend them. Below, I discuss five harms that flow directly from policies and laws justified by the Myth.

A. Overbroad Laws

Congress typically responds to the Myth of the Superuser by passing broad laws. Generally, lawmakers broaden criminal and civil prohibitions, giving law enforcement agencies sweeping new authorities even though these can be used (and are used) against non-Superusers.

In short, Congress overreacts. They fear an American version of Onel de Guzman, the Philippines citizen who confessed to writing the

[89] *See* Green, *supra* note 50. Clarke is not alone in his exaggeration. "Digital Pearl Harbor" was not coined by him and it has been used by many over the past decade and a half. *Id.* Other similar worry-phrases include "electronic Chernobyl," "digital Armageddon," and "digital Waterloo." *See id.*

"ILOVEYOU" Virus but escaped punishment because Philippines law did not criminalize the type of harm he had caused.[90]

Furthermore, legislators tend to respond to the Myth by focusing on statutory *conduct* elements rather than result, harm, intent, or attendant circumstance elements.[91] This makes sense. Conduct is what makes the Superuser unusual, and the power they wield is often what some find offensive or threatening.[92] For example, § 1030(a)(5)(A)(i) of the CFAA prohibits "caus[ing] the transmission of a program, information, code, or command." This sweeping phrase seems to encompass sending any data over the Internet. It applies to all sorts of perfectly nonthreatening acts that ordinary users perform every day.

Consider the following. In 2000, Bret McDanel worked for a company that supplied email and voicemail accounts.[93] He revealed an internal security vulnerability to his employers, but they ignored him.[94] After leaving his job, McDanel sent an email message through his former employer's computer system in which he revealed the vulnerability to 5600 of the company's customers.[95] The U.S. Attorney prosecuted McDanel for violating § 1030(a)(5)(A).[96]

[90] *See* Bryan Glick, *Cyber Criminals Mock the Archaic Legal Boundaries*, COMPUTING, Jan. 4 2001, at 32.

[91] In the Model Penal Code's vocabulary, the elements of a criminal statute come in four separate flavors: conduct, results or harm, intent, and attendant circumstances. *See* MODEL PENAL CODE § 1.13(9) (2001) (classifying conduct elements into conduct, attendant circumstances, and results). For example, under 18 U.S.C. § 2252A(a)(5)(B) (2000) it is a crime to possess images of child pornography. Parsing this prohibition into the four MPC categories:

> [a]ny person who . . . knowingly [(intent)] possesses [(conduct)] any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography [(results/harm)] that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer [(attendant circumstances)].

18 U.S.C. § 2252A(a)(5)(B).

[92] This bias applies even against those who use Superuser power benignly or for morally or ethically good outcomes. *See infra* Part II.C.

[93] *See* Chris Sprigman, *The Federal Government's Strange Cyber-Defamation Case Against Bret McDanel: A Prosecution that Should Never Have Been Brought*, FINDLAW, Sep. 25, 2003, http://writ.news.findlaw.com/commentary/20030925_sprigman.html.

[94] *See id.*

[95] *See id.*

[96] *See id.*

The prosecution's only plausible theory must have been that McDanel's email messages amounted to "a program, information, code, or command," despite that the phrase usually applies to things like computer viruses and worms.[97] The U.S. Attorney's interpretation arguably met the plain text, because email messages are literally "information."[98] Perhaps if Congress had been less fearful of the Superuser, it could have drafted a more circumscribed, specific statute that would not have applied to McDanel's acts.[99] Instead, McDanel served one year and four months in prison.[100] After he appealed, the DOJ confessed error and dropped McDanel's conviction.[101]

Like the overbroad language targeting conduct, § 1030(a)(5)(A)(ii) prohibits "access[ing] [a protected computer] without authorization."[102] "Access" is not defined, and neither is "without authorization." Many courts have interpreted these vague terms broadly.[103]

[97] *See id.*

[98] There is a second, perhaps more egregious, problem with such a theory. Only those who commit "damage" are guilty of violating this provision. *See* 18 U.S.C. § 1030(a)(5)(A)(i) (2000 & Supp. V 2005). Damage is defined broadly, again perhaps as a reaction to the Superuser, to include "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8). The prosecution allegedly argued that the damage caused was McDanel's employer's reputation. *See* Sprigman, *supra* note 93.

[99] To be sure, it is imaginable, especially to one persuaded by the Myth of the Superuser, that some Superuser criminal could use email messages to attack a system, for example, as part of a Denial of Service attack. *See generally* JELENA MIRKOVIC ET AL., INTERNET DENIAL OF SERVICE: ATTACK AND DEFENSE MECHANISMS (2004) (discussing Denial of Service attacks in depth). Even those who disagree with the prosecution of McDanel might argue the conduct element should be broad to encompass this hypothetical criminal. I contend that those making this argument have fallen prey to the Myth of the Superuser. Even though this potential harm is covered by the broad conduct element, that coverage comes at a cost of other harms from overbreadth, as discussed below.

[100] *See* Sprigman, *supra* note 93.

[101] The government's concession involved the damage element, not the conduct element discussed here. *See* 18 U.S.C. § 1030(a)(5)(A)(i). In its motion to reverse the conviction, the government conceded that "[o]n further review, in light of defendant's arguments on appeal, the government believes it was error to argue that defendant intended an 'impairment' to the integrity of Tornado's computer system." Government's Motion for Reversal of Conviction at 3-4, United States v. McDanel, No. 03-50135 (9th Cir. Oct. 14, 2003), *available at* http://www.lessig.org/blog/archives/govt.pdf.

[102] 18 U.S.C. § 1030(a)(5)(A)(ii).

[103] Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1617 (2003) (noting "several recent decisions point toward remarkably expansive interpretations of unauthorized access").

Consider this example stemming from a civil lawsuit.[104] A travel agency had an employee write a computer program to collect, or "scrape" its competitor's prices from a website.[105] The competitor sued, alleging a violation of the "access to defraud" provision of the CFAA, which relies on the aforementioned broad terms, "access" and "authorization."[106] Although the defendants had merely accessed a public website to copy publicly available information, the First Circuit Court of Appeals held that they exceeded authorized access because they arguably violated a confidentiality agreement between the plaintiff and one of its former employees.[107] In other words, this broadly worded computer hacking and fraud statute proscribed mere contract breach.

As a result of Congress's expansion of these prohibitions, conduct is no longer a meaningful, limiting principle for many federal computer crimes. Because the Superuser's conduct is hard to define, Congress has given up trying to do so. So long as you merely "transmit" or "access," you have satisfied the conduct elements of the crime. These elements have become low hurdles that, when cleared, place ordinary users' benign acts within the general reach of the prohibitions.[108] In McDanel's case, the broad prohibitions meant sixteen months of wrongful imprisonment.

The harm worsens with time. Each new hypothetical threat or vague anecdote adds to the toolbox that Superusers are said to possess. Lawmakers apply a ratchet to laws like § 1030, broadening substantive provisions and increasing criminal penalties with nearly every Congress.[109] They are spurred on by law enforcement officials asking

[104] The CFAA permits civil lawsuits for people harmed by the same prohibited acts that are criminal under § 1030. 18 U.S.C. § 1030(g). Professor Kerr has noted the spillover effect these civil lawsuits have on interpretations of criminal prohibitions, as courts may be more inclined to entertain novel, aggressive theories of civil liability that they might reject in the criminal context. *See* Kerr, *supra* note 103, at 1641-42 n.210.

[105] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579-80 (1st Cir. 2001).

[106] 18 U.S.C. § 1030(a)(4); *EF Cultural Travel BV,* 274 F.3d at 581.

[107] *EF Cultural Travel BV*, 274 F.3d at 582 (analyzing evidence in light of preliminary injunction standard).

[108] Other commentators have written about this feature of computer crime law, but they are split about whether it is desirable. *Compare* Kerr, *supra* note 103, at 1647-48 (arguing for expansive interpretation of "access" within § 1030, placing greater weight on meaning of "authorization"), *with* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2254 (2004) (advocating for narrower meaning for access as "the more natural" reading).

[109] The Senate Report on the 1996 amendments to the Act states:

for help tackling new threats on the horizon.[110] Meanwhile, once-innocent behavior begins to fall into new classes of prohibited conduct.

Broad statutes are not only a problem when they lead to the conviction of the inculpable. They also raise civil liberties concerns by enabling what I call "investigatory overbreadth." Broad conduct elements lead to enormous suspect pools. Imagine there has been an attack on a corporate web server. Because the court in the travel agency website dispute[111] construed "without authorization" to apply to those who merely breach contractual duties, the acts of all employees and contractors must be scrutinized.[112] Because the *McDanel* court held that email messages to third parties constituted the "transmission of information," the private email messages or instant messages of customers and other outsiders should also be scrutinized.[113]

Thus, investigatory overbreadth refers to how broad conduct elements place no limit on the number or type of people who are suspects.[114] Compounding the problem, broad conduct elements make it easier for police to establish probable cause to search the belongings of suspects. This is further exacerbated by the fact that most Internet surveillance laws do not require notice to the party

> As computers continue to proliferate in businesses and homes, and new forms of computer crime emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse Act statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime.

S. REP. NO. 104-357, pt. 2, at 5 (1996); *see also* United States v. Middleton, 231 F.3d 1207, 1212 (9th Cir. 2000) (stating "Congress has consciously broadened [§ 1030] since its original enactment").

[110] *See supra* note 18 (listing major revisions to § 1030).

[111] *See supra* notes 102-103 and accompanying text.

[112] *See supra* note 105.

[113] *See supra* note 93.

[114] A related trend is the creation of laws that punish the possession or use of a particular technology, rather than the harm caused by the technology. *See* Joseph M. Olivenbaum, *Ctrl-Alt-Delete: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 575-76 (1997) (explaining that "[t]o the extent that [computer crime laws] focus on technological means, rather than on the harm caused by a defendant's conduct, those statutes tend towards overbreadth by sweeping within their ambit anyone who uses the means regardless of result"); Douglas Thomas, *Criminality on the Electronic Frontier: Corporality and the Judicial Construction of the Hacker, in* CYBERCRIME: LAW ENFORCEMENT, SECURITY, AND SURVEILLANCE IN THE INFORMATION AGE 18 (Douglas Thomas & Brian D. Loader eds., 2000).

surveilled.[115] Thus, law enforcement officials could read the email messages and obtain the browsing habits of dozens or more people without jeopardizing the investigation. The combination of broad prohibitions and low surveillance standards gives the police both the incentive and the means to cast out larger and more invasive dragnets.

Suppose that in our web server hypothetical, Congress had clarified that certain crimes could be conducted only by outsiders.[116] In this situation, the pool of suspects would have been significantly smaller. Likewise, this would be the case if Congress had clarified that "transmitting information" did not apply to mere email communications, contra *McDanel*.[117] Congress, however, is loath to narrow conduct elements, not because it is convinced that insiders or people like McDanel deserve punishment, but more likely because it worries that a Superuser's acts will slip outside a narrow prohibition. But is the possibility of a highly unlikely criminal evading conviction through a loophole worse than routinely investigating and prosecuting people like McDanel for seemingly innocent acts?

B. Unduly Invasive Search and Seizure

Part of what is terrifying about the Superuser is how the Internet allows him to act anonymously. He can hop from host to host and country to country with impunity. To find the Superuser, the police need better search and surveillance authorities, better tools, and the latitude to pursue creative solutions for piercing anonymity.

But broad search authorities can be used unjustifiably to intrude upon civil liberties. Search warrants for computers are a prime example, because the judges who sign and review these warrants

[115] *See* 18 U.S.C. § 2511(2)(a)(ii)(B) (2000) (forbidding providers from "disclos[ing] the existence of any interception or surveillance" conducted pursuant to court order under Wiretap Act and providing civil damages for failing to comply); *id.* § 2703(c)(3) (2000 & Supp. V 2005) (dispensing with notice requirement under Stored Communications Act for government access, with appropriate process, to "records or information" about subscriber); *id.* § 3123(d)(2) (2000 & Supp. V 2005) (similar provision for pen registers and trap and trace devices). *But see id.* § 2703(b)(1)(B) (2000) (requiring "prior notice" for access to certain types of subscriber content information); *id.* § 2705 (2000) (providing mechanism for delaying notice required by § 2703).

[116] *Cf. id.* § 1030(a)(3) (2000) (defining criminal attacks on government systems to exclude certain insiders); *id.* § 1030(a)(5)(A)(i) (2000 & Supp. V 2005) (defining nonaccess attacks on protected computers to apply only to one "without authorization" but omitting, by implication, insiders who act "in excess of authorization").

[117] *See supra* note 93.

usually authorize sweeping and highly invasive searches justified by storytelling about a particular species of Superuser we might call the "Data Hider."

Agents seeking computer search warrants consider it standard practice to tell stories in supporting affidavits about the sophisticated technology that can be used to hide data.[118] According to this boilerplate, criminals are known to use steganography,[119] kill switches,[120] and encryption to hide evidence of their crimes.[121] These agents also assert that file names and extensions are almost meaningless, because users can easily change this information to hide data.[122] These assertions are important, because courts have repeatedly held that each file in a computer is a separate "container" over which a person has a reasonable expectation of privacy under the Fourth Amendment and for which the police must usually establish independent probable cause to open.[123]

Convinced of the prowess of the Data Hider, a typical judge will usually sign a warrant that authorizes (1) the search of every single file on subject computers, (2) the search of hard drive parts that do not even store files,[124] and (3) offsite searches, where data is

[118] *See* U.S. DEP'T OF JUSTICE, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm [hereinafter DOJ MANUAL] (offering model search warrant that includes language to justify offsite search: "Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and recover 'hidden,' erased, compressed, encrypted or password-protected data.").

[119] Steganography is defined and discussed *infra* in Part IV.B.1.d.

[120] Kill switches are commands or hardware devices that can be triggered to cause the deletion of data. *See* Timothy Roberts, *Protecting Against Digital Data Thefts with a 'Kill Switch,'* SAN JOSE BUS. J., Dec. 30, 2005, *available at* http://sanjose.bizjournals.com/sanjose/stories/2006/01/02/story5.html.

[121] *See, e.g.*, United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915, 961 (9th Cir. 2006) (assessing search warrant affidavit that spun tales about users mislabeling files, using encryption, and using steganography).

[122] File extensions are the parts of file names that, by convention, reveal the broad type of data stored within. On Windows computers, these extensions are usually the last three letters of the file name, following the final dot. For example, "SuperuserArticle.doc" has an extension of ".doc." The ".doc" extension signifies that the file is a Microsoft Word document. But any user can change the filename to mask the extension, making the Word document, for example, appear to be an MP3 music file.

[123] *See* United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999); Kerr, *supra* note 45, at 554-57.

[124] These areas of "latent data" are often unknown to most computer users. Some examples include the swap file, deleted space, file slack, and RAM slack. *See* Kerr,

forensically examined for months or maybe even years.[125] In upholding the scope of these searches, reviewing courts make bare and broad proclamations about what criminals do to hide evidence.[126] These broad pronouncements are built upon nothing more than the agent's assertions and the judge's intuitions about computer technology.

For example, the Ninth Circuit Court of Appeals has held that "[c]omputer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent."[127] To support this claim, the Ninth Circuit quoted a district court opinion from Vermont,[128] which in turn cited a district court opinion from Florida.[129] The Florida court based its conclusion about data tampering on what an agent said he had been told by a Customs Service forensic computer expert.[130] Such is the path from the Myth of the Superuser to binding court of appeals case law.

In reality, if criminals tend not to hide data inside obscured file names or unusual directories, judges might feel compelled to ask the police to cordon off parts of a computer's hard drive.[131] The law

supra note 45, at 542 (stating that "[c]omputers are also remarkable for storing a tremendous amount of information that most users do not know about and cannot control").

[125] *See* United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) (upholding search warrant that allowed blanket search through all files on hard drive); United States v. Adjani, 452 F.3d 1140, 1150 (9th Cir. 2006) (same).

[126] *See Hill*, 459 F.3d at 978 (finding that "[c]riminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer"); *Adjani*, 452 F.3d at 1150 (stating that "[c]omputer files are easy to disguise or rename, and were we to limit the warrant to such a specific search protocol, much evidence could escape discovery simply because of Adjani's (or Reinhold's) labeling of the files documenting Adjani's criminal activity . . . [t]he government should not be required to trust the suspect's self-labeling when executing a warrant").

[127] *Hill*, 459 F.3d at 978.

[128] United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998).

[129] United States v. Abbell, 963 F. Supp. 1178, 1199 (S.D. Fla. 1997).

[130] *Id.*

[131] In a dissenting opinion, Judge Fisher of the Ninth Circuit, who wrote *Adjani*, seemed to argue for requiring this kind of additional proof, albeit in an atypical context, that is, in a case involving the criminal investigation arising from the Major League Baseball "BALCO" steroid scandal. United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915, 919-20 (9th Cir. 2006). Judge Fisher opined that the government had "made misleading statements in . . . search warrant applications," in part because "[t]he government did not have any evidence or reason to believe that CDT had engaged in steganography, boobytrapping computers, or any type of data destruction or alteration." *Id.* at 961.

enforcement community fears such a result.[132] It prefers instead to use computer forensics tools that treat the hard drive as a unitary pool of data through which to search.[133]

So where does this particular myth end and reality begin? Common sense suggests that some criminals are paranoid enough to hide evidence. But it is also highly improbable that all criminals are likely to use these tactics. Home computer users committing relatively nontechnological crimes — death threats or extortion via email, for example — may have less incentive to hide evidence and no access to the tools required to do so. Painting all criminals in every warrant application as uniformly capable of hiding information is a classic example of the Myth.

In accepting the bare assertion that every computer user is a potential Data Hider, judges may fail to uphold the Fourth Amendment rights of those searched. In some cases, constraints on the allowable scope of the search of a hard drive may be sensible and even constitutionally mandated.[134]

[132] *See* DOJ MANUAL, *supra* note 118, § II.C (stating, "[f]or example, it is generally unwise to limit a search strategy solely to keyword searches"); Kerr, *supra* note 45, at 576 (explaining "[t]he computer forensics process calls for ex-post standards, not ex-ante rules").

[133] *See* Kerr, *supra* note 45, at 538. This is not to say that computer forensics could not be executed in a more limited, privacy-sensitive manner. If a court signed a warrant that required the police to avoid particular parts of a hard drive, forensics experts would be able to use most of their tools to do this kind of analysis. *See* Brief of Amici Curiae Computer Forensics Researchers and Scientists in Support of Appellant and Reversal of the Denial of the Motion to Suppress at 22, United States v. Andrus, No. 06-3094 (10th Cir. June 1, 2007), 2007 WL 3264595, at *22 (brief co-authored by this Article's author) ("Furthermore, [the commonly used computer forensics tool] EnCase makes it possible to create a filter to exclude specified parts of the hard drive from review: a forensic technician merely needs to click on specific folders from among all of the folders on the hard disk to include them and only them in an operation.").

[134] For example, in a search of a hard drive for evidence of music illegally distributed over peer-to-peer networks, it may make sense to limit the search to the computer directories used by that particular type of peer-to-peer software. Just as a warrant to search for a gun cannot be used to support a search through stacks of paper on a desk, *cf.* United States v. Ross, 456 U.S. 798, 820 (1992) ("A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found . . . ."), agents should not be allowed to look for music where it cannot be found. *Compare* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) (upholding scope of computer search because agent "searched for relevant records in places where such records might logically be found. . . . [He] selectively proceeded to the 'Microsoft Works' sub-folder on the premise that because Works is a spreadsheet program, that folder would be most likely to contain records relating to the business of drug trafficking"), *with* United States v. Carey, 172 F.3d 1268, 1274 (10th Cir.

Allowing computer-wide searches in every case dramatically impinges on privacy. As hard drive capacity grows, the incentive for computer users to delete old files diminishes.[135] Today's computers can contain tens of thousands of letters, email messages, business records, and financial documents, stretching back years.[136] In the computer context, courts have interpreted the plain view rule to mean that evidence of any crime found during a computer search can be used to prosecute the computer's owner, even if it is unrelated to the crime recited in the warrant.[137] Commentators have likened hard drive-wide searches to the general warrants that incensed the Founding Fathers.[138] Even if this is not a perfect comparison, these searches are the closest thing to general warrants that we have in modern police practice. By succumbing to the Myth, judges have given the police the power to search at odds with Fourth Amendment protections.

C. Guilt by Association

Another harm results when policymakers confuse power and evil. This mistake is borne of a flawed syllogism: Power can be used online to cause harm, Superusers are powerful, and therefore, Superusers are harmful. This ignores the fact that many Superusers cause no harm and may even cause great benefit. As a result of this flawed view, benign or beneficial Superusers are branded illicit, and in the extreme case, they are sued or prosecuted for doing nothing except wielding

1999) (suppressing evidence found on computer because after finding one image of child pornography, "[w]hen he opened the subsequent [similarly named] files, he knew he was not going to find items related to drug activity as specified in the warrant"). Obviously, if law enforcement agents have any particularized reason to suspect that this music distributor is likely to obscure data, the affidavit should reflect this fact, and the warrant should allow more scrutiny of the hard drive.

[135] *Cf.* Paul Festa, *Google to Offer Gigabyte of Free E-mail*, CNET NEWS.COM, Apr. 1, 2004, http://www.news.com/Google-to-offer-gigabyte-of-free-e-mail/2100-1032_3-5182805.html?tag=item (explaining that "Google will offer enough storage so that the average email account holder will never have to delete messages").

[136] *See* Kerr, *supra* note 45, at 541-42 ("Computer hard drives sold in 2005 generally have storage capacities . . . roughly equivalent to . . . the amount of information contained in the books on one floor of a typical academic library.").

[137] *See id.* at 576-77.

[138] *See id.* at 566 ("Narrowing or even eliminating the plain view exception may eventually be needed to ensure that warrants to search computers do not become the functional equivalent of general warrants.").

their power.[139] This is guilt by association of an especially pernicious and illogical form.

Felten, a professor of Computer Science and Public Affairs at Princeton University, has suffered from this kind of overreaction. Felten's research focuses on DRM and computer security, using especially applied methods to actively try to circumvent software security to expose flaws.[140] Under threat of a lawsuit, Felten was once forced to delay presenting his research.[141] He now consults regularly with lawyers before undertaking sensitive projects and consuming time and energy better spent on research.[142]

D. Wasted Investigatory Resources

Because Superusers can evade detection and identification, they are difficult to find. In my opinion, while the DOJ does a very good job of capturing and punishing dim hackers, the smart ones tend to get away. Given enough money, time, and tools, law enforcement agencies could catch some Superusers, but with the same resources, they could find many more non-Superusers instead.

Even though law enforcement tends primarily to capture non-Superuser criminals, the DOJ raises the specter of the Superuser criminal whenever it discusses computer crime with Congress.[143]

[139] *See supra* note 114.

[140] *See, e.g.*, Posting of Ed Felten to Freedom to Tinker Blog, http://www.freedom-to-tinker.com/?p=975 (Feb. 14, 2006, 09:19) (summarizing DRM research on Sony rootkit).

[141] *See* John Markoff, *Scientists Drop Plan to Present Music-Copying Study That Record Industry Opposed*, N.Y. TIMES, Apr. 27, 2001, at C5.

[142] Letter from Edward W. Felten & J. Alex Halderman, Princeton Univ., to Office of the Gen. Counsel, U.S. Copyright Office 7 (Dec. 1, 2005), *available at* http://www.freedom-to-tinker.com/doc/2005/dmcacomment.pdf ("Researchers like Professor Edward Felten and Alex Halderman waste valuable research time consulting attorneys due to concerns about liability under the DMCA.") (responding to Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472 (Nov. 27, 2006) (to be codified at 37 C.F.R. pt. 201)).

[143] *See, e.g.*, *The Cyber Security Enhancement Act of 2001: Hearing on H.R. 3482 Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 107th Cong. (2002) (statement of John G. Malcolm, Deputy Assistant Att'y Gen. of the United States), *available at* http://www.cybercrime.gov/HR3482_01Testimony.htm (describing Russian hackers and citing CSI/FBI statistics); *Department of Justice's Efforts to Fight Cybercrime: Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary*, 107th Cong. (2001) (citing statement of Michael Chertoff, Assistant Att'y Gen. of the United States), *available at* http://www.cybercrime.gov/cybercrime61201_MChertoff.htm (describing hackers from Russia and Eastern Europe, cyberterrorists,

Congress often responds by increasing the resources and tools at the DOJ's disposal, focusing on the hardest cases, which probably represent a small fraction of the victims and harm.[144]

E. The Myth and Legal Scholarship

Scholars too often fall prey to the Myth.[145] By doing this, at the very least, they shift attention away from the proper heart of most online debates — the problems posed by ordinary users. Worse, the prescriptions arising from these Myth-based arguments are often fundamentally flawed.

Consider again the DRM debate. Scholarly critics of DRM point to a paper written by four Microsoft engineers, entitled *The Darknet and the Future of Content Distribution*, as proof of the ineffectiveness of laws like the Digital Millennium Copyright Act ("DMCA").[146] The first premise of the *Darknet* paper is the sentence most often misused: "Any widely distributed object will be available to a fraction of users in a form that permits copying."[147] In other words, in the battle between lock builders and lock pickers, the *Darknet* authors assume that the lock-picking Superusers have the upper hand.

Legal scholars who cite this proposition often miss the fact that it is merely an assumption.[148] The *Darknet* paper authors do not prove the assumption with rigor, but instead take it as a starting point. Others,

attacks on critical infrastructures, and dubious statistics).

[144] *See supra* Part I.A.2 (describing Congress's approach to modifying CFAA).

[145] *See infra* notes 146-59 (discussing legal scholars' use of so-called "darknet" hypothesis). Student note authors seem to fall prey to the Myth more often than their counterparts in the professorial ranks. *See, e.g.*, Stephen W. Tountas, Note, *Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?*, 11 WASH. U. J.L. & POL'Y 351, 376 (2003) ("Given the devastation of September 11, along with sophisticated tactics such as steganography, it is in Congress'[s] best interest to disregard Carnivore's constitutional issues" (footnote omitted)). It may be that student authors are more careless or prone to logical missteps in their analyses. On the other hand, it may be that student authors are more aware of advanced technology and more willing to consider the implications of the use of advanced technology.

[146] *See* Peter Biddle et al., *The Darknet and the Future of Content Distribution* (2002), *available at* http://crypto.stanford.edu/DRM2002/darknet5.doc. The scholar most associated with bringing the *Darknet* paper into mainstream legal scholarship is Fred von Lohmann. Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures*, 24 LOY. L.A. ENT. L. REV. 635, 641 (2004).

[147] Biddle et al., *supra* note 146, at 2.

[148] *Id.*

however, have cited the first premise of the *Darknet* paper as proven fact,[149] which it is not.[150]

Compounding the problem, those who cite the first premise tend to misread exactly what it says. The first premise is a statement about possibilities, not inevitabilities.[151] The authors do not (nor could they) contend that the world's Superusers have the skill, time, and interest to crack every single piece of DRM-protected content. Theirs is a more modest point about incentives, studded with caveats: only works that are "widely distributed" satisfy the claim; only a "fraction of users" can copy these works; even vulnerable works that "permit" copying will not necessarily be copied.[152]

The *Darknet* paper, in sum, supports several propositions at odds with the conventional scholarly perception of the paper. First, DRM-protected copies of unpopular music may never be broken, because no Superusers will unlock them. Likewise, because of what I call the "limits of human bandwidth,"[153] — the idea that Superusers break DRM at a fixed rate — even protection schemes used for popular music may have to wait in line for an interested Superuser to come along.[154] For some content owners, DRM systems that remain unbroken for months or years are good enough.[155] This is especially true because users can always be convinced or forced to upgrade to

[149] *See* Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing*, 17 HARV. J.L. & TECH. 1, 9-10 (2003); von Lohmann, *supra* note 146, at 640.

[150] The reason the *Darknet* paper authors felt no need to prove the first premise is because their aim was to comment on what happens after Superusers have acted. Their central argument was that small, informal, closed-but-interconnected networks can efficiently distribute libraries of copyrighted works that "approach the aggregate libraries that are provided by the global darknets [such as the peer-to-peer networks] of today." Biddle et al., *supra* note 146, at 9. Yesterday's tight-knit circles of cassette-swapping teenagers have been replaced by larger groups with fast Internet connections, complex software, powerful computers, and giant hard drives. So long as some Superusers feed these darknets (again, this is just an assumption), these darknets will thrive and be very difficult to detect and shut down. People who cite the *Darknet* paper often mistake the starting point for the conclusion. *See* Netanel, *supra* note 149, at 9-10; von Lohmann, *supra* note 146, at 640.

[151] *See* Biddle et al., *supra* note 146, at 2.

[152] *Id.*

[153] *See infra* note 241 and accompanying text (discussing limits of human bandwidth).

[154] *See* Nate Anderson, *Hacking Digital Rights Management*, ARS TECHNICA, July 18, 2006, http://arstechnica.com/articles/culture/drmhacks.ars (noting that Microsoft's DRM system for audio "has not been widely breached" since late 2001).

[155] *See id.* (noting that even imperfect DRM schemes "may be good enough for most [record] labels").

newer, stronger versions of DRM.[156] In fact, despite how it is portrayed and regarded in the scholarly community, the *Darknet* paper is surprisingly optimistic about certain aspects and types of DRM. For example, the authors note that "[e]xisting DRM-systems typically provide protection for months to years."[157] In other words, DRM is often good for a few months' head start.

To be sure, the *Darknet* paper casts serious doubts on the ability of DRM to stop all copyright infringement. The authors try to temper expectations that laws like the DMCA will be a "silver bullet" against the spread of unauthorized copies of copyrighted works.[158] Thus, in the debate over DRM, the paper stands squarely on the side of those who doubt DRM's status as a panacea.

Nevertheless, the paper's conclusions have been overstated by scholars tempted by the Myth. The sound-bite version of the paper's conclusion is the claim that powerful users will circumvent any protection scheme released.[159] This sound bite is intuitive, appealing, and wrong.[160]

[156] *See* Randal C. Picker, *Rewinding Sony: The Evolving Product, Phoning Home and the Duty of Ongoing Design*, 55 CASE W. RES. L. REV. 749, 766-68 (2005); Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 2019 (2006).

[157] In the conclusion to the paper, the authors go so far as to say that if darknets tend to be isolated from one another (a possibility the authors implicitly seem to doubt), then some particularly weak classes of DRM "are highly effective." Biddle et al., *supra* note 146, at 15.

[158] However, the *Darknet* paper authors are optimistic about the law's ability to disrupt aspects of digital copyright infringement. In fact, the paper appears to have been written in response to the success of lawsuits against centrally run services such as Napster, Gnutella, and Kazaa. *See id.* at 5-8. The paper seems decidedly pessimistic about the ability of such centralized services to resist legal challenges for long. *See id.* at 7-8. Even the DMCA is called a "far-reaching (although not fully tested) example of a law that is potentially quite powerful." *Id.*

[159] *See* Netanel, *supra* note 149, at 9 (citing *Darknet* paper, along with another source, for proposition that, "[i]n fact, computer security experts maintain that no technological barrier can ultimately prevail over determined hackers who have physical access to the encrypted items").

[160] The *Darknet* paper is a good model of a measured, careful way of dealing with the Superuser. In its last section, the paper calls for further empirical work about the nature of the darknets, consistent with my recommendation for a more searching empirical inquiry to back up Superuser claims in Part IV. *See* Biddle et al., *supra* note 146, at 15 (stating that "[i]t appears that quantitative studies of the effective 'diffusion constant' of different kinds of darknets would be highly useful in elucidating the dynamics of DRM and the darknet").

III. MYTH ORIGINS AND PERPETUATION

Why is it so difficult to assess Superuser risks — to measure the power and reach Superusers command? There are three parts to the answer, which together describe a pervasive fear-processing machine.

The machine operates on fear, and in particular, a documented, widely held fear of the Internet.[161] We fear the Internet for both rational and irrational reasons; our fears are created or magnified by the media. Just-so stories about imaginable (but implausible) new powers that evil Superusers may wield are fed into the machine, which in turn spits out miscalculated risks, misguided advocacy, poor policymaking, and the litany of harms outlined in Part II.

So far, this is a fairly conventional account, as the basic connection between fear and risk assessment is well-known in the social science literature. Specifically, the literature surveyed in Part III.A identifies heuristics and biases which lead us to miscalculate risk when faced with fear. These heuristics and biases are the valves, gears, and bearings of the fear-processing machine. Although this conventional account can explain, in part, the Myth of the Superuser, I extend and challenge the literature by focusing on two much more idiosyncratic features of the Internet's fear-processing machine.

The first variation from the conventional account stems from the malleability of software. Software is easy to change in fundamental ways, but those who fall prey to the Myth of the Superuser misinterpret or misuse this fact. As I discuss in Part III.B, although software is malleable, many observers have confused the possible with the inevitable, partly because they have been confused by Professor Lessig's thoughts about code. Misunderstandings about the malleability of software feed new stories of fear and risk to the machine at a rate rarely seen with real world stories.

Second, I focus on experts, the machine's operators. In other situations, experts try to temper public fear to slow the machine's output to a manageable rate. With online risk, the machine is unmanned. As Part III.C explains, even experts cannot assign probabilities to online risks.

Taken together, these features — fear, code malleability, and expert abandonment — turn the conventional account into a much more troubling one. It becomes more difficult to remedy and a more pressing a concern than analogous problems offline. To begin the assessment, I start with fear.

[161] *See infra* Part III.A.1.b.

A. Myth Origins: Fear

1. Fear

During the past thirty-five years, sociologists and psychologists have developed an extensive literature about fear, focusing in particular on human responses to fear and the effect of those responses on decision-making.[162] Scholars have recently imported this literature into theories of law, particularly with respect to environmental risks, such as global warming.[163] To date, no one has applied this fear and risk literature to Internet regulation. This approach holds great promise, in light of both the widely held and well-documented fear of the Internet as well as the pre-eminence of rhetoric and storytelling in policy debates about online regulation.

a. The Effects of Fear

Fear causes laypeople and policymakers to exaggerate some risks and to downplay others in spite of the actual probability that those risks will occur. In *Laws of Fear*, Cass Sunstein surveys psychological and sociological explanations.[164] Sunstein focuses on two as particularly important: the availability heuristic and probability neglect.[165]

The availability heuristic is the psychological tendency to give greater weight to scenarios one can imagine.[166] The heuristic is triggered primarily with risks that are both familiar and salient.[167] Familiar risks are those we can readily imagine.[168] Because the risks from smoking are more familiar than the risks from sunbathing, Sunstein notes, people are more likely to exaggerate the risk from

[162] *See generally* HEURISTICS AND BIASES: THE PSYCHOLOGY OF INTUITIVE JUDGMENT (Thomas Gilovic, Dale Griffin, & Daniel Kahneman eds., 2002) (collecting important papers in heuristics and biases scholarship); JUDGMENT UNDER UNCERTAINTY: HEURISTICS AND BIASES 3, 11-14 (Daniel Kahneman, Paul Slovic, & Amos Tversky eds., 1982) (same); PAUL SLOVIC, THE PERCEPTION OF RISK (2000) (examining disconnect between expert measurements of risk and public perception of risk).

[163] *See* CASS SUNSTEIN, LAWS OF FEAR: BEYOND THE PRECAUTIONARY PRINCIPLE 36 (2005).

[164] *See id.* at 35-49.

[165] *See id.*

[166] *See id.* at 36-39.

[167] *See id.* at 37.

[168] *See id.*

smoking.[169] Salient risks trigger a similar reaction. Viewing a house fire, for example, is likely to have more impact than reading about it in the newspaper because of the saliency of witnessing the fire firsthand.[170]

Probability neglect is the tendency to pay little attention to the probability of a risk occurring, often experienced with worst case or emotionally charged risks.[171] The risk of death from airplane crashes, for example, tends to trigger stronger reactions than the other, more likely causes of death because of probability neglect.[172] Sunstein notes that "when intense emotions are engaged, people tend to focus on the adverse outcome, not on its likelihood."[173]

b. *Fear of the Internet*

The widely held fear of the Internet connects these observations to the Myth of the Superuser. Prior literature demonstrates a strong connection between fear and new technology.[174] In perhaps the most comprehensive summary of studies about information technophobia, Professor Mark Brosnan reports large segments of the population suffer from some fear of computer technology.[175]

Repeated surveys spotlight people's fear of the Internet. A survey commissioned by the U.K. government found that "[f]ear of [I]nternet crime is now more prevalent than concerns about more conventional crimes such as burglary, mugging and car theft."[176] In a 2003 survey,

[169] *See id.*

[170] *See id.* (citing Amos Tversky & Daniel Kahneman, *Judgment Under Uncertainty: Heuristics and Biases*, *in* JUDGMENT UNDER UNCERTAINTY, *supra* note 162, at 3, 11-14).

[171] *See id.* at 39-41.

[172] *See id.* at 39-40. Sunstein notes that the availability heuristic also plays a role in this particular example. *See id.* at 40. The availability heuristic will cause a person to think airplane crashes are more likely to occur than their actual incidence, while probability neglect will cause people to ignore the probability of an airplane crash completely. *See id.* at 39.

[173] *Id.* at 64; *see also id.* at 40 (explaining that "vivid images of disaster . . . crowd[] out probability judgments").

[174] *See, e.g.*, MARK J. BROSNAN, TECHNOPHOBIA: THE PSYCHOLOGICAL IMPACT OF INFORMATION TECHNOLOGY 10-36 (1998) (summarizing studies about extent of fear of information technology).

[175] *Id.* at 12. Brosnan cites studies, for example, finding 50% of college students registering as technophobic. *Id.* (citing Larry D. Rosen & Phyllisann Maguire, *Myths and Realities of Computerphobia: A Meta-Analysis*, 3 ANXIETY RESEARCH 175 (1990)).

[176] *See* Helen Carter, *Internet Crime Eclipses Burglary in Survey of Perceived Risks*, THE GUARDIAN, Oct. 9, 2006, http://www.guardian.co.uk/technology/2006/oct/09/news.crime.

the Pew Internet and American Life Project discovered that 49% of Americans fear that terrorists might cripple American utilities, banks, or corporations through cyberattacks.[177] Two years earlier, the same organization discovered that over 70% of Americans were "concerned" or "very concerned" about child pornography, credit card theft, hackers, and organized terrorism online.[178]

We fear the Internet on several levels. First, we fear that the world is becoming less comprehensible to the average person. We fear that increasing technological complexity masks a terrifying fragility: the world seems one cascading failure away from becoming unplugged, taking away all of the essential services we have migrated online in the past decade.[179]

Second, we fear malicious Superusers on the Internet for several reasons. We imagine the Internet teeming with all kinds of evildoers, from simple predators to "Supercriminal" Superusers, such as organized crime figures, terrorists, and war fighters.[180] Worse, they have tools unlike any seen before; even everyday Internet applications like email and the web are used to perpetrate frauds and harm children with terrifying efficiency.[181] These tools are nothing compared to the more powerful and more inscrutable ones we fear they wield.[182] While it would be hard to claim that the fear of

[177] MEMORANDUM FROM LEE RAINIE, PEW INTERNET & AM. LIFE PROJECT, SURVEY WITH FEDERAL COMPUTER WEEK MAGAZINE ABOUT EMERGENCIES AND THE INTERNET 1 (Aug. 31, 2003), *available at* http://www.pewinternet.org/pdfs/PIP_Preparedness_Net_Memo.pdf.

[178] PEW INTERNET & AM. LIFE PROJECT, FEAR OF ONLINE CRIME: AMERICANS SUPPORT FBI INTERCEPTION OF CRIMINAL SUSPECTS' EMAIL AND NEW LAWS TO PROTECT ONLINE PRIVACY 9 (2001), *available at* http://www.pewinternet.org/pdfs/pip_fear_of_crime.pdf (showing over 70% of Americans "concerned" or "very concerned" about child pornography, credit card theft, hackers, and organized terrorism online).

[179] *See* TAYLOR, *supra* note 29, at xiii ("Conversely, fear of computer technology complements our perennial cultural concern that we cannot ultimately control our technological curiosity."). Paul Taylor links the fear of computer technology to "the historical range of cultural expressions that give [the fear] voice," citing Prometheus and Icarus, *Frankenstein*, to more modern examples including *Neuromancer*, *Blade Runner*, and *Terminator*. *Id.*

[180] *Id.* ("We are fascinated by the 'black box' nature of computers and the technical virtuosity of hackers who manipulate them, but at the same time we are fearful of their lack of transparency and the fact that our conventional concept of technological experts may be fatally undermined by largely anonymous, unaccountable, and potentially subversive technological whiz-kids.").

[181] *See generally* PHISHING AND COUNTERMEASURES: UNDERSTANDING THE INCREASING PROBLEM OF ELECTRONIC IDENTITY THEFT (Markus Jakobsson & Steven Myers eds., 2006) (tracing history of so-called Phishing attacks, in which attackers use email and fraudulent websites to steal identities).

[182] In particular, the fear of anonymity is pronounced. TAYLOR, *supra* note 29, at

technology lacks any rational basis[183] (after all, technology often fails in spectacular, frightening ways), the amount of fear and anxiety we feel about the Internet is difficult to justify.[184]

The fear of the Internet can trigger the availability heuristic and probability neglect, explaining in part, but not in whole, the tendency to exaggerate the power of the Superuser. It might seem odd that something as intangible and technologically complex as the Internet would trigger the availability heuristic, which focuses on the familiar and salient; yet the availability heuristic still exerts great influence for at least three reasons.

First, although the causes or mechanisms of online risk are sometimes bogged down in technical detail, they result in tangible, easy-to-imagine effects. Planes fall out of the sky, power grids go dark, children are stalked, and credit card numbers are stolen. Second, the media report on online risks incessantly.[185] Third, nearly everyone has suffered firsthand from some form of online harm. Computer viruses, hard drive crashes, and spam have become a constant part of our daily, online existence. Perhaps experiences with these kinds of minor harms cause people to miscalculate the likelihood of severe types of online harm. "I am sure hackers can break into defense department networks," the reasoning might go, "because my computer seems to get a new virus every day."

xiii ("One of the main factors making hacking particularly suitable for media hyperbole is its aura of anonymity.").

[183] A rich literature describes the technophobia associated with any perceived risk from new technology. *See* Levi, *supra* note 22, at 50.

[184] Focusing on public concerns about privacy, Kim Taipale, executive director of the Center for Advanced Studies in Science and Technology Policy, advances a similar theory, and points the finger at many sources.

> The availability of information privacy horror stories (in particular, the prevalence of identity theft, spam and hacker stories in the media), and the general mistrust in government agencies to handle personal information appropriately, combined with a general apprehension about technology and how it works, and the natural anxiety relating to disclosure of personal, particularly intimate, information — all spurred on by the privacy lobby — has created a public anxiety about electronic privacy out of proportion to the actual privacy risks and has obscured discussion of the very real threats posed by either failing to provide security or by misallocating security resources.

K.A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd*, 7 YALE J.L. & TECH. 123, 137-38 (2004-2005) (footnotes omitted).

[185] *See infra* Part III.A.2.

Similarly, fear of the Internet triggers probability neglect. Many harms online are the type of worst case, emotionally charged harms that trigger inattention to probabilities.[186] Child pornography and cyberterrorism, in particular, supply the public with easy-to-visualize, horrific, and even apocalyptic imagery.[187] As a result of probability neglect and the availability heuristic, observers imagine there are many Superusers when in reality there are few, or they believe that Superusers have a much stronger impact or reach than they actually do.[188]

2. Superusers in the Media

It is also useful to examine the relationship between the media and fear. The media pays a lot of attention to Superusers. This may be a simple effect of the Myth, or it may be a root cause.

Some sociologists believe the media causes fear.[189] According to these theories, the media exaggerates and overemphasizes stories about risks to maximize ratings and readership, which exacerbates the public's fear.[190] Although this so-called "media-effects theory" is contested,[191] regardless of its validity, many agree that the media pays

[186] *See* Cass R. Sunstein, *Probability Neglect: Emotions, Worst Cases, and Law*, 112 YALE L.J. 61, 76 (2002) ("My central claim is that when strong emotions are involved, large-scale variations in probabilities will matter surprisingly little — even when the variations unquestionably matter when emotions are not triggered.").

[187] *See* Green, *supra* note 50 (recounting predictions of impending "digital Armageddon" resulting from cyberterrorism).

[188] Another way to characterize this phenomenon involves the types of logical mistakes caused from the biases of fear. Logicians call this mistake the hasty generalization or the converse accident. *See* NICHOLAS BUNNIN & JIYUAN YU, THE BLACKWELL DICTIONARY OF WESTERN PHILOSOPHY 250 (2004) (explaining entry for "fallacy of *secundum quid*"). This informal logical fallacy undermines inductive reasoning from a particular case to a general rule. *Id.* When the specific cases are not numerous enough or typical enough to illuminate the general rule, drawing the latter from the former is an error. *See id.*

[189] *See generally* SUNSTEIN, *supra* note 163, at 87 ("[N]ews sources do a great deal to trigger fear . . . ."); Ronald Weitzer & Charis Kubrin, *Breaking News: How Local TV News and Real-World Conditions Affect Fear of Crime*, 21 JUST. Q. 497, 497 (2004) (examining "the role of the media in shaping crime fears, in conjunction with both demographic factors and local crime conditions").

[190] LORI DORFMAN & VINCENT SCHIRALDI, BUILDING BLOCKS FOR YOUTH, *Off Balance: Youth, Race & Crime in the News* (2001), *available at* http://www.buildingblocksforyouth.org/media/media.html (describing how media portrayals of crime can drive public policy responses and frame issues for public).

[191] *See* BARRY GLASSNER, THE CULTURE OF FEAR: WHY AMERICANS ARE AFRAID OF THE WRONG THINGS 26-29 (1999); Karen Frost et al., *Relative Risk in the News Media: A Quantification of Misrepresentation*, 87 AM. J. PUB. HEALTH 842, 844 (1997); David Gauntlett, *Ten Things Wrong with the "Effects Model"* (1998), *available at*

disproportionate attention to sensational stories aimed at fear-inducing topics.[192] The Superuser is an example: he is a pervasive image, especially compared to the exaggerated focus on online crimes committed by unsophisticated non-Superusers.

News stories about online threats appear regularly in major newspapers.[193] Many of these stories exaggerate the sophistication of the crimes and the criminals. Consider, for example, convicted hacker Kevin Mitnick. By some accounts, Mitnick is the most notorious computer hacker in the world.[194] Mitnick's forte was "social engineering," a glorified term for skillful lying.[195] He once obtained proprietary source code and manuals from a Pacific Bell field office by convincing the person at the front desk of a data center that he was an employee.[196] Most of his infamous attacks relied on social engineering, not technical wizardry.[197]

http://www.theory.org.uk/david/effects.htm.

[192] *E.g.*, DORFMAN & SCHIRALDI, *supra* note 190 (surveying various print and broadcast news sources spanning nearly 100 years and concluding "[t]he news media report crime, especially violent crime, out of proportion to its actual occurrence").

[193] Consider the following headlines that appeared in the *New York Times* in 2006: Associated Press, *Computer Hackers Attack State Department*, N.Y. TIMES, July 12, 2006, at A6; Associated Press, *Hackers Gain Data on AT&T Shoppers*, N.Y. TIMES, Aug. 30, 2006, at C2; William L. Hamilton, *You're Not Alone*, N.Y. TIMES, Nov. 23, 2006, at F1 (describing threat to networked home computers as "the next frontier of risk"); Metro Briefing/New Jersey, *Newark: University Computers Hacked*, N.Y. TIMES, Apr. 10, 2006, at B4; Alex Mindlin, *Your Computer Is Under Attack — LOL*, N.Y. TIMES, Feb. 20, 2006, at C3; David Shenk, *A Growing Web of Watchers Builds a Surveillance Society*, N.Y. TIMES, Jan. 25, 2006, at G6; Tom Zeller, Jr., *Cyberthieves Silently Copy Your Passwords as You Type*, N.Y. TIMES, Feb. 27, 2006, at A1.

[194] *See* Michael Specter, *An Ex-Con Logs On*, NEW YORKER, Feb. 3, 2003, at 32 (stating "Mitnick . . . is usually described as the world's most notorious hacker"); Patricia Jacobus, *Mitnick Released from Prison*, CNET NEWS.COM, Mar. 24, 2001, http://www.news.com/Mitnick-released-from-prison/2100-1023_3-235933.html (noting "Kevin Mitnick, one of the world's most notorious computer hackers").

[195] In his post-prison, reformed public persona, Mitnick has even written a few books about social engineering. *See, e.g.*, KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF DECEPTION: CONTROLLING THE HUMAN ELEMENT OF SECURITY (2002) (exploring how hackers use social engineering); KEVIN D. MITNICK & WILLIAM L. SIMON, THE ART OF INTRUSION: THE REAL STORIES BEHIND THE EXPLOITS OF HACKERS, INTRUDERS & DECEIVERS (2005) (describing real-life stories of computer intrusions, many involving social engineering).

[196] *See* KATIE HAFNER & JOHN MARKOFF, CYBERPUNK 50-51 (1991).

[197] *See id.*; Elizabeth Weise, *Hacker Prowess Exaggerated? Computer Villain Seen as Virtually Marginal in Reality*, CHARLOTTE OBSERVER, Jan. 27, 1996, at 2A (explaining that "in news reports, Mitnick was pictured as a lone, master hacker, capable of doing almost anything with a computer or even just a phone. In reality, Mitnick's technical skills were only fair").

Despite the low-tech methods Mitnick used, some in the media have portrayed him as a technical genius.[198] A *New York Times* article written at his arrest breathlessly announced that "[t]he technical sophistication of the pursued and his pursuer . . . was remarkable."[199]

In addition to these newspaper accounts, authors have written many books about the lore of the Superuser hacker.[200] The pervasive attention to the Superuser extends beyond print media. The lone, genius hacker has become almost a stock figure in many movies, such as *WarGames*, *The Matrix*, *TRON*, and *Sneakers*.[201]

The media's exaggeration of technical sophistication is a shame, because careful media attention can dispel the Myth and provide a calming influence on public fears. For example, three praiseworthy articles in the *New York Times* in 2006 sought to defuse, not heighten, the Myth of the Superuser. One story described the realization by officials at ChoicePoint, a prominent data broker, that despite all of its efforts to harden its computer databases, unscrupulous "customers" were buying information under the cover of legitimate businesses.[202] Another

[198] *See* Associated Press, *Cyberspace Raider to Get Plea Bargain*, ATLANTA J. & CONST., July 2, 1995, at A5 (calling Mitnick "[a] computer hacker with a history of breaking into some of the nation's most protected computer systems"); Bernard Levin, *Misappliance of Science*, TIMES (U.K.), Mar. 24, 1995, at 16 (listing crimes attributed to Mitnick to conclude that "this man is a genius," and "Mitnick, it is very clear, could clean out a thousand bank systems and retire with countless billions of dollars").

[199] John Markoff, *Hacker and Grifter Duel on the Net*, N.Y. TIMES, Feb. 19, 1995, at A1. By "pursuer," Markoff is referring to Tsutomo Shimomura, a computer researcher who helped find Mitnick. Granted, the article goes on to mention that "[i]f anything, Mr. Mitnick's real 'darkside' brilliance comes not from his computer skills, but from his insight into people." *Id.* After Mitnick's arrest, Markoff and Shimomura co-authored a book, JOHN MARKOFF & TSUTOMO SHIMOMURA, TAKE-DOWN: THE PURSUIT AND CAPTURE OF KEVIN MITNICK, AMERICA'S MOST WANTED COMPUTER OUTLAW — BY THE MAN WHO DID IT (1996). Reportedly the marketing copy for the book referred to Mitnick as "a hacker who 'could have crippled the world.'" Greg Miller, *Did Reporter Sensationalize Case?*, SEATTLE TIMES, Mar. 20, 1999, at A2.

[200] *See generally* HAFNER & MARKOFF, *supra* note 196 (profiling several famous computer hackers); JONATHAN LITTMAN, THE FUGITIVE GAME: ONLINE WITH KEVIN MITNICK (1996) (describing pursuit and arrest of Mitnick); MARKOFF & SHIMOMURA, *supra* note 199 (same); BRUCE STERLING, THE HACKER CRACKDOWN (1992) (describing arrest of Mitnick); CLIFFORD STOLL, THE CUCKOO'S EGG (1989) (detailing pursuit of computer intruders).

[201] Others deemed merely footnote-worthy include *The Matrix* sequels (Warner Bros. 2003), HACKERS (Metro-Goldwyn-Mayer 1995), THE NET (Columbia Pictures 1995), SWORDFISH (Warner Bros. 2001), JOHNNY MNEMONIC (Sony Pictures Home Entertainment 1995), GOLDENEYE (Metro-Goldwyn-Mayer 1995), THE LAWNMOWER MAN (New Line Cinema 1992), EXISTENZ (Alliance Atlantis 1999), and ANTITRUST (Metro-Goldwyn-Mayer 2001).

[202] Gary Rivlin, *Keeping Your Enemies Close*, N.Y. TIMES, Nov. 12, 2006, § 3 at 1.

article tried to spotlight the difference between "data breach" and "identity theft," concepts that are often conflated by the media.[203] A third article argued that when it comes to stolen data and identity theft, "[h]ackers and sophisticated data thieves are one thing. But in the battle to stop the great hemorrhaging of personal data, the enemy is us."[204]

Thus, conventional social science explains many of our observations about the Myth of the Superuser. Fear, abetted by the media spotlight, causes people to rely on the availability heuristic and to suffer from probability neglect. Both phenomena lead to exaggerated risk assessments.

B. Myth Origins: Technology

Heuristics and biases explain why we exaggerate the online fears we have, but they cannot so easily explain why exotic, new, online fears develop so rapidly, and why the number and variety of myths seem so plentiful compared to other fields. Why are new fears added so quickly to the Internet's fear-processing machine? The way to account for this is to look at the nature of the technology; networks, software, and hardware are malleable, but only to an extent. Due to confusion about Lessig's ideas about code, this malleability is too often mistaken for boundless possibility.

1. Malleability, or the Care and Feeding of Superusers

Superusers thrive by taking advantage of several well-known features of programmers, code, computers, and networks. First, Superusers benefit from the openness of software and hardware.[205] Computer hardware is almost always shipped in an easy-to-open case that invites tinkering, even though most computer users will never tinker.[206] Computer software is sold in a metaphorically similar manner, with the typical operating system ("OS") shipped to allow "administrator access" by the average user.[207]

[203] Steve Lohr, *Surging Losses, But Few Victims*, N.Y. TIMES, Sept. 27, 2006, at G1.

[204] Tom Zeller, Jr., *93,754,333 Examples of Data Nonchalance*, N.Y. TIMES, Sept. 25, 2006, at C5.

[205] *See* Zittrain, *supra* note 156, at 1982-87.

[206] *See generally* WINN L. ROSCH, THE WINN L. ROSCH HARDWARE BIBLE (6th ed. 2003) (providing detailed guide for repairing and understanding personal computer hardware).

[207] *See* Zittrain, *supra* note 156, at 1983 ("Most significant, PCs were and are accessible. They were designed to run software not written by the PC manufacturer or OS publisher, including software written by those with whom these manufacturers

These are not mandatory design choices. Hardware could be shipped sealed and inaccessible, and the OS could allow only limited control.[208] Were those choices the status quo, it would be harder to be a Superuser.[209] This is why experts modify and adapt the open PC much more easily than the closed, hard-to-modify TiVo.[210]

Second, networks are also open to scrutiny and manipulation.[211] Although openness is why the Internet has so grown rapidly to include many innovative services, it can be exploited by the Superuser. For example, robust authentication controls — mechanisms to verify that a person online is who they say they are — were not designed into the Internet's core protocols.[212] Although authentication has been added after the fact, the unauthenticated core is always there.[213] Thus, Superusers can take advantage of the network's trust to act undetected.

Third, software will always be imperfect. All commercial software programs have bugs[214] because it would be too expensive to drive them all away.[215] Superusers find and exploit these bugs to

had no special arrangements.").

[208] Microsoft has trumpeted the fact that its latest version of Windows, Vista, makes nonadministrator access the default. *See* Posting of Jim Allchin to Windows Vista Team Blog, http://windowsvistablog.com/blogs/windowsvista/archive/2007/01/23/security-features-vs-convenience.aspx (Jan. 23, 2007, 17:32).

[209] *See* Zittrain, *supra* note 156, at 1982-87; *cf.* Jay Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 NOTRE DAME L. REV. 583 (2006) (explaining how defaults operate in software and how policymakers should set defaults).

[210] *See* Zittrain, *supra* note 156, at 2014-15.

[211] *See* Mark Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925, 930 (2001) ("It is the view of many in the Internet community, ourselves included, that the extraordinary growth of the Internet rests fundamentally upon its design principles. Some of these principles relate to the openness of the Internet's standards and the openness of the software that implemented those standards.").

[212] *Cf.* KIM CAMERON, THE LAWS OF IDENTITY (2005), *available at* http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (discussing why it is hard to add identity to Internet).

[213] *See* David Talbot, *The Internet is Broken*, TECH. REV., Dec. 20, 2005, *available at* http://www.technologyreview.com/Infotech/16051/page2/ ("Simply put, the Internet has no inherent security architecture — nothing to stop viruses or spam or anything else. Protections like firewalls and antispam software are add-ons, security patches in a digital arms race.").

[214] Crispin Cowan, Calton Pu, & Heather Hinton, *Death, Taxes, and Imperfect Software: Surviving the Inevitable*, *in* ACM PROCEEDINGS OF THE 1998 WORKSHOP ON NEW SECURITY PARADIGMS 54, 55 (1998) ("Commercial software chronically has bugs, many with security vulnerability implications.").

[215] *See id.* "Tempting as it may be to hypothesize that this is because the vendors are lazy or stupid, this is not the case. Commercial software chronically has bugs for

circumvent security, break DRM, or otherwise cause software to do what it is not designed to do.[216]

Finally, programmers — often Superusers themselves — purposefully enable expert level control frequently. Consider, for example "command line" programs such as UNIX shells or the Windows command prompt.[217] With these programs (which are quite homely by today's graphical standards), users key in esoteric commands to control the OS, for example, to copy files, create folders, or run programs.[218] Although they can do these things with a modern graphical user interface, experienced command line users consider themselves more efficient than their mouse-bound counterparts.[219]

2. Misunderstanding "Code Is Law"

Relying on Lessig's important work on code for support, people mistakenly interpret the Internet's malleability to mean limitless possibility for Superuser power.[220] Lessig famously spotlighted the role that software plays in regulating online behavior.[221] Easily modifiable software, Lessig noted, defines the "laws of nature" of online spaces.[222] If a programmer decides he wants people to "walk through walls" online, he can change the code to allow that behavior. In this way, software regulates online conduct in much the same way laws (and norms and markets) do.[223] In slogan form, "Code is Law."[224]

the dual-reason that correctness is hard, and correctness does not sell software." *Id.*; *see also* Eric Sink, *Why We All Sell Code with Bugs*, GUARDIAN UNLIMITED, May 25, 2006, at 6, *available at* http://www.guardian.co.uk/technology/2006/may/25/insideit.guardianweeklytechnologysection.

[216] Brad Stone, *A Lively Market, Legal and Not, for Software Bugs*, N.Y. TIMES, Jan. 30, 2007, at A1 (describing "the willingness of Internet criminals to spend large sums for early knowledge of software flaws that could provide an opening for identity-theft schemes and spam attacks").

[217] *See* NEAL STEPHENSON, IN THE BEGINNING . . . WAS THE COMMAND LINE 13 (1999) (describing command lines).

[218] *See* JERRY PEEK, GRACE TODINO, & JOHN STRANG, LEARNING THE UNIX OPERATING SYSTEM 11-14 (5th ed. 2002) (describing basic UNIX commands).

[219] *See* STEPHENSON, *supra* note 217, at 74. Stephenson describes how Apple programmers created a command line interface on the early Macintosh computer — the symbol of the birth of the graphical user interface — "so that they would be able to get some useful work done."

[220] *See infra* notes 225-27 and accompanying text.

[221] LESSIG, *supra* note 7 *passim*.

[222] *Id.* at 24.

[223] *See id.* at 125.

[224] *Id.* at 1.

Unfortunately, few have accepted Lessig's important and useful insights as an invitation to study the malleability of code in a rigorous way. Legal academics, in particular, have embraced the general idea that code is important, but they too often treat it as mysterious and complex — a hopeless moving target.[225] The tendency is to hope that code will evolve to resolve conflicts, an unrealistic technological determinism.[226] Worse, others fall into a "science fiction trap," imagining that every kind of new technology is possible.[227] By ignoring the constraints of reality, these people can make any problem melt away. The truth, however, is not so rosy.

In particular, the misinterpretation of Lessig's ideas has led to what I call "metaphor failure." Internet law is often a battle of metaphors. When reading my email messages, is my ISP acting more like the postman who glances at the backs of postcards or the one who rips

[225] *See* R. Polk Wagner, *On Software Regulation*, 78 S. CAL. L. REV. 457, 492 (2005) ("[S]oftware development is a rapidly moving, nearly unpredictable target, making it difficult to directly address software through legal regulation."). I do not mean to be too critical of Professor Wagner's article, because although I think he overemphasizes the unpredictability and instability of code development, the article stands as a leading example of a careful analysis of law's effect on code. His overemphasis on the instability of code causes him to offer prescriptions that are much too deferential, but this is a critique of fine points while celebrating the article's larger goals.

[226] There is an ancient (in network terms) famous mantra that exemplifies this point: "[T]he [Inter]net interprets censorship as damage and routes around it." *See* GOLDSMITH & WU, *supra* note 6, at 3 (quoting John Gilmore). Except sometimes the Internet does not route around censorship, and censorship flourishes. James Fallows, '*The Connection Has Been Reset*,' ATLANTIC MONTHLY, Mar. 2008, *available at* http://www.theatlantic.com/doc/200803/chinese-firewall (describing China's use of firewalls and other Internet technology to monitor and block disfavored traffic).

[227] Lessig himself has occasionally been guilty of falling for the science fiction trap, most conspicuously by placing too much stock in the Platform for Privacy Preferences ("P3P"). P3P is a form of so-called "intelligent agents," little pieces of software which might automate and mediate our privacy wishes with the websites we visit. In *Code*, Lessig argued that "with a technology like P3P, we could lower transaction costs enough to make a property rule [instead of a liability rule] work." LESSIG, *supra* note 7, at 229. As Lessig himself noted in the 2006 version of the book, his recommendation to propertize privacy has been criticized. *Id.* at 383 n.47 (citing critics). Lessig's vision of the P3P protocol — easy to use, easy to deploy, rich enough to contain our preferences but simple enough to be understandable — assumes away many difficult technical problems. *See* ELEC. PRIVACY INFOR. CTR & JUNKBUSTERS, PRETTY POOR PRIVACY: AN ASSESSMENT OF P3P AND INTERNET PRIVACY (2000), http://epic.org/reports/prettypoorprivacy.html ("[P3P] is a complex and confusing protocol that will make it more difficult for Internet users to protect their privacy.").

open closed envelopes?[228] Is an encrypted document more like a paper letter inside a closed box or a shredded document?[229]

Superusers' actions seem more science fiction than reality. As one scholar noted, "What is talked about, in terms of hackers at least, is the manner in which hackers themselves exist in a shadowy space of secrecy, possessing near mystical powers that allow control of technology that itself is beyond discourse."[230] A hacker can pass through "impenetrable" firewalls[231] (walk through walls), install a rootkit[232] (leave behind no trace), scan entire networks in search of interesting files in a matter of minutes[233] (fly through entire neighborhoods of information), and walk off with millions of identities (thousands of pages of information) never to be heard from again (vanish).

When metaphors for online concepts fail, scholars and policymakers become deeply unmoored. Stripped of comparison points, they see online conflicts as blank slates. These conflicts provide opportunities to rewrite rules and start from scratch, propose creative and untested solutions, and abandon ordinary tools that have been used for decades in real world conflicts. This is a form of an Internet exceptionalist strain of thinking that many scholars have debunked in recent years but that stubbornly persists among policymakers and even some

[228] *See* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 365-68 (2003).

[229] *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 884 (1995).

[230] Thomas, *supra* note 114, at 27.

[231] *See* Byron Acohido & Jon Swartz, *Unprotected PCs Can Be Hijacked in Minutes*, USA TODAY, Nov. 29, 2004, at 3B (finding that "firewalls, which restrict online access to the guts of the PC operating system, represent a crucial first line of defense against cyberintruders").

[232] Rootkits are programs, typically installed by computer intruders that wipe out traces of the intruder's identity from the computer's security detection systems. *See* Paul Roberts, *RSA: Microsoft on 'Rootkits': Be Afraid, Be Very Afraid*, COMPUTERWORLD, Feb. 17, 2005, *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,99843,00.html (describing new, more threatening rootkit technologies).

[233] *See* J.D. Biersdorfer, *Q&A: From a Crisp Web Image to a Blur, via the Printer*, N.Y. TIMES, Sept. 6, 2001, at G4.

> A port scan means that another computer on the Internet is looking for an open door to your machine. Port scans are legal and are used in some cases for network management and administration, but hackers are also increasingly using port scanning to find a way to break in so that they can tamper with the computer or steal data from it.

Id.

academics.[234] To these people, imagining the possibility of a harm is enough; confirming such speculation with people with firsthand (or even secondhand) experience is optional.

We are better off once we realize that although code is malleable, it is also constrained and predictable. Code can and will change, but at least within a short time frame, it will only do so in certain ways. Mindful of the many constraints on software, we can make better predictions, and avoid and dispel misguided thoughts about the endless power of the Superuser.

3. The Truth About Code: Constraints, Not Endless Possibility

There are many constraints on the evolution and development of software. First, there are constraints of technology. Software can do only what is permitted by hardware and other software. Programs cannot interact with the physical world in futuristic, fantastic ways unless a piece of hardware facilitates that type of interaction.[235] Application programs cannot manipulate files unless the OS allows it to do so.[236]

Of course, given the generativity of computers, constraints of technology are surmountable with time and money.[237] This suggests the second, closely related constraint: the constraint of organization. Despite the romantic vision of the lone programmer, toiling away on the "Great American Program," most of the software we use every day was written by a large committee.[238] Although wealthy, large corporations can finance complex products, their resources are not

[234] *See, e.g.*, Timothy Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 682 (2003); James Grimmelman, Note, *Regulating by Software*, 114 YALE L.J. 1719, 1728-30 (2005). I also made this point in a student note. Paul Ohm, Note, *Usenet: On Regulating the Internet*, 46 UCLA L. REV. 1941, 1957 (1999).

[235] It is not enough to simply have the right piece of hardware. Some hardware will be constrained, again by software. For example, device drivers are small pieces of critically important software that allow an operating system to interact with specific bits of hardware. *See* Zittrain, *supra* note 156, at 2018.

[236] *See* NEMETH ET AL., *supra* note 9, at 73-74 (describing UNIX operating system's file permissions methods).

[237] *See* Zittrain, *supra* note 156 *passim* (using label "generativity" to describe malleability of hardware and software).

[238] *See* FREDERICK P. BROOKS, THE MYTHICAL MAN MONTH: ESSAYS ON SOFTWARE ENGINEERING 31 (20th anniv. ed. 1995) (reporting that at peak, 1000 people worked simultaneously to support creation of Operating System OS/360); *cf.* STEVEN WEBER, THE SUCCESS OF OPEN SOURCE 59 (2004) (noting that most software written by one person "is used only by the author or perhaps a few friends").

limitless; internal politics, inertia, and other similar "frictions" also limit the type and pace of innovation they are likely to achieve.[239]

The market serves as another organizational constraint. Although small tools are often developed to scratch a particular developer's idiosyncratic itch, larger products often need a market to emerge.[240] Market forces channel developers away from the outlandishly new in favor of gradual change instead.

Finally, software is written by people who toil under constraints of human fallibility. People tend to be busy, distracted, and unorganized.[241] They make mistakes and often lack imagination.[242] Witness the web browser. Despite more than a decade of innovation, the web browser continues to impart information essentially as it did at its invention with pages full of text and graphics (and in the principal subsequent innovation, the occasional video clip) scrolling up and down the screen.[243]

The limits of human bandwidth serve as another form of human fallibility, one that is perhaps even more important than the failure of imagination. The average programmer can keep only a small amount of code straight in her head and thus can produce only a modest amount of new code daily.[244] Consequently, a finite number of programmers — for example, Superuser DRM circumventors — can

[239] *See* WEBER, *supra* note 238, at 57-65 (describing "problem" of developing complex software). Even Open Source software is subject to this constraint. Any reasonably complex, widely used Open Source project — Linux, Firefox, Apache, MySQL — required the work of dozens or more programmers to achieve the stability and feature set of a mature product. *See id.* at 94-127 (describing development of Linux, Apache, and Mozilla). Tales from the trenches describe internecine battles and outright schisms (explaining code fork, to use a technical phrase) in the development of some of these products. *Id.* at 64.

[240] *But see* YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 41-48 (2006) (describing increasing importance of nonmarket drivers in information industries).

[241] *Cf.* BROOKS, *supra* note 238, at 30 (reporting statistics about difference in productivity between best and worst computer programmers).

[242] William S. Curran, *The Outer Limits of Programming, in* PROCEEDINGS OF THE 38TH ACM SOUTHEAST REGIONAL CONFERENCE, 2000, at 38, 38 (commenting that human computer programmers "have limits to our mental capacities").

[243] *See* Andrew Orlowski, *Browser Innovation is Dead — Andreessen*, THE REGISTER, July 2, 2003, http://www.theregister.co.uk/2003/07/02/browser_innovation_is_dead_andreessen/ (quoting Marc Andreessen, inventor of Mosaic and Netscape browsers, "there hasn't been any innovation on the browser in the last five years").

[244] Curran, *supra* note 242, at 38 (noting that 50 lines of code is both supposed "practical limit [of] the number of lines [of programming code] that a typical programmer can keep clearly in his/her head" as well as upper bound of what "average programmer produces . . . daily").

produce only a finite output.[245] Whether a particular new DRM scheme is attacked and successfully circumvented, then, depends on the aggregate priorities of a number of people.

The power of these constraints varies depending on the interval of time about which predictions are being made. Over a long time horizon — say ten or twenty years — these constraints will have minimal effect on the evolution of software. Over the short term, these constraints dominate, and software tends to evolve, not lurch.[246]

If we view claims of Superuser power through the lens of these constraints — technology, organization, and human fallibility — we can separate the probable from the merely possible. In a world of endless possibility, Superusers can do anything online. But in reality, many would-be Superusers will try to hack software and fail, lack the imagination or expertise to succeed, or look for co-conspirators and find none. Then having failed, they will move on to the next project, other diversion, or day job.

C. Myth Perpetuation: The Failure of Expertise

What I have described so far is a fear-processing machine fed with stories about all-powerful Superusers, supplied at an amplified rate due to misunderstandings about the malleability of code, and acted upon by well-known heuristics and biases we suffer in the face of fear. The final piece is the machine's operator. Most of Sunstein's examples involve risks with well-known probabilities calculated by experts.[247] These experts regulate the knobs and dials of the machine, trying to slow the output to a manageable rate. The problem with online risk is that even experts have trouble assigning meaningful probabilities to different risks because the machine is unattended. How often will a hacker successfully breach a server? How often does unlawful access

[245] *Id.* ("Now let's consider a program estimated to require, say, ten million lines of code. At ten lines per day, that would take a thousand programmers a thousand days. That's about four years of work for the thousand programmers.").

[246] In the terms of evolutionary biology, software evolves through phyletic gradualism, not punctuated equilibrium. *Cf.* THOMAS KUHN, THE STRUCTURE OF SCIENTIFIC REVOLUTIONS (1962) (introducing concepts of paradigm shifts); Niles Eldredge & Stephen Jay Gould, *Punctuated Equilibria: An Alternative to Phyletic Gradualism*, *in* MODELS IN PALEOBIOLOGY 82 (Thomas J.M. Schopf ed., 1972) (introducing theory of punctuated equilibrium), *available at* http://www.blackwellpublishing.com/ridley/classictexts/eldredge.asp.

[247] *E.g.*, SUNSTEIN, *supra* note 163, at 96-97 (discussing risk of contracting SARS in Canada); *id.* at 117 (discussing risks of harm from cell phone radiation and arsenic in drinking water); *id.* at 132-36 (describing various calculations of value of statistical life).

to a social security number result in identity theft? Experts rarely ask these types of questions.

Contrast Sunstein's paradigmatic experts: scientists who assess the risks of cancer, the safety of nuclear power plants, or the dangers of genetically modified foods.[248] These researchers rigorously analyze statistics to calculate risks.[249] In fact, the disconnect between their focus on numbers and probabilities and the average person's seeming disregard for statistics is a central mystery pursued in *Laws of Fear*.[250]

In stark contrast, experts in the field of computer crime and computer security seem uninterested in probabilities. Why are experts in this field willing to abdicate the important risk-calculating role played by their counterparts in other fields? Consider the following four explanations.

1. Pervasive Secrecy

Online risks are shrouded in secrecy. Software developers use trade secret law and compiled code to keep details away from public consumption.[251] Computer hackers dwell in a mythical, shadowy underground and trade vulnerabilities in private chat rooms.[252] Security consultants are contractually bound not to reveal the

[248] *Id.* at 139 (describing studies on eliminating cancer risks); *id.* at 47 (discussing expert evaluations of risk from nuclear power plants); *id.* at 40 (discussing concerns about genetically modified organisms).

[249] *Id.* at 139.

[250] This is not to say that Sunstein and the social scientists he cites find all expert risk assessment flawless. At one point, Sunstein concedes that experts tend to "use their own heuristics and have their own biases." *See id.* at 86-87 (citing SHELDON RAMPTON & JOHN STAUBER, TRUST US, WE'RE EXPERTS! (2001)). He does not, however, spend much time on this observation, nor does he point out any situations in which experts seem to have the very same biases as nonexperts. *See also* Kahneman & Tversky, *supra* note 170, at 18 (explaining that "[t]he reliance on heuristics and the prevalence of biases are not restricted to laymen . . . [e]xperienced researchers are also prone to the same biases — when they think intuitively").

Kahneman and Tversky (and probably Sunstein) seem to be talking about exceptional instances where experts fall prone to biases despite their training and rigor. The studies they cite, for example, focus on problems that are "more intricate" and "less transparent" than the "elementary errors" made by laypeople. *Id.* at 18. In contrast, I claim that experts of online risk tend to make precisely the same mistakes of judgment as made by laypeople.

[251] *See* WEBER, *supra* note 238, at 192. "[C]ontrol of the source code is the foundation of [the traditional software] business model. . . . The simplest way to retain control is to give only the binary executable codes to the customer." *Id.* The obvious exception to this tendency is the Open Source model. *Id.*

[252] *See* Thomas, *supra* note 114, at 27.

identities of those who hire them.[253] Law enforcement agencies refuse to divulge statistics about the number, type, and extent of their investigations and resist congressional attempts to increase public reporting.[254]

Since the September 11 attacks, the secrecy culture surrounding code has broadened. The government has introduced new secrecy measures with the goal of protecting our nation's communications networks, now part of the governmentally defined "Critical Infrastructure."[255] For example, industry experts and government officials meet periodically to share information about online risks in a so-called Information Sharing and Analysis Center; those discussions are not made available to the public.[256]

2. Everybody Is an Expert

The world abounds with computer experts, simply because theirs is a title too easily obtained. All you need is skill with a computer; formal training and background in rigorous methods are not required. In fact, to many of these anointed experts, most academic types —

[253] *See* Levi, *supra* note 22, at 46.

[254] When Congress passed the update to the USA PATRIOT Act, known as the USA PATRIOT Improvement and Reauthorization Act of 2005, it sought to increase congressional oversight, by requiring additional auditing and reporting to Congress about the government's uses of certain FISA authorities. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 106, 119, 120 Stat. 278, 199-200 (2006). President George W. Bush issued a signing statement to the new law, reserving the right not to comply with the new requirements. President George W. Bush, *President's Statement on H.R. 199, the "USA PATRIOT Improvement and Reauthorization Act of 2005"* (Mar. 9, 2005), *available at* http://www.whitehouse.gov/index.html (search "President's Statement on H.R. 199, the 'USA PATRIOT Improvement and Reauthorization Act of 2005'"; then click on first hyperlink). The statement said, in pertinent part:

> The executive branch shall construe the provisions of H.R. 3199 that call for furnishing information to entities outside the [E]xecutive [B]ranch, such as sections 106A and 119, in a manner consistent with the President's constitutional authority to supervise the unitary executive branch and to withhold information the disclosure of which could impair foreign relations, national security, the deliberative processes of the Executive, or the performance of the Executive's constitutional duties.

Id.

[255] *See* NATIONAL STRATEGY, *supra* note 86, at 13-14.

[256] *See* Kevin Poulsen, *Feds Urge Secrecy over Network Outages*, SECURITYFOCUS, June 23, 2004, http://www.securityfocus.com/news/8966 ("Data exchanged within the Telecom-[Information Sharing and Analysis Center] is protected from public disclosure.").

those likeliest to conduct rigorous risk assessments — are, in fact, inexpert because they focus too much on theory over practice.[257]

Part of this stems from the garage hacker history of computer innovation.[258] Unlike modern medicine, where most important advances require money and years of formal education to achieve, many computer breakthroughs come from self-taught tinkerers.[259] Generally, this democratizing nature of online expertise would be cause for celebration.

The problem is that self-educated computer experts tend to have neither the training nor inclination to approach problems statistically and empirically. People may be called before Congress to testify about identity theft or network security, even if they have no idea nor even care how often these risks occur.[260] Their presence on a speakers' list crowds out the few academics who are thinking about these things empirically and rigorously.[261]

[257] For example, in reporting news that Microsoft had opened a new research facility in Cambridge, Massachusetts, the *New York Times* quoted many sources that suggested a divide between theoretical computer science and "useful" "product development." Katie Hafner, *Microsoft Adds Research Lab in East as Others Cut Back*, N.Y. TIMES, Feb. 4, 2008, at C3; *cf.* Robert L. Glass, *Revisiting the Industry/Academe Communication Chasm*, 40 COMM. ACM 11, 13 (1997) (fearing "communication chasm between [computer science] academe and industry" which are "unnecessary because both academics and practitioners are typically bright and rational people who share similar goals").

[258] *See* PAUL FREIBERGER & MICHAEL SWAINE, FIRE IN THE VALLEY: THE MAKING OF THE PERSONAL COMPUTER 78-79, 118-24 (2d ed. 1999) (describing role of hobbyists and enthusiasts in establishing market for PCs); Zittrain, *supra* note 156, at 1984-85 (discussing role of hobbyists in development of commercial software); Posting of Howard Rheingold to Huridocs-Tech, Human Rights Education Associates, (Dec. 23, 1999), *available at* http://www.hrea.org/lists/huridocs-tech/markup/msg00383.html.

[259] *See* Walter Isaacson, *Thinkers vs. Tinkerers, and Other Debates*, TIME, Mar. 29, 1999, at 6 (comparing "relative influence of thinkers vs. tinkerers" over time, and focusing in particular on role of tinkerers in computing advances).

[260] For example, a subcommittee of the House Judiciary Committee recently held a hearing to discuss identity theft. *Privacy and Cybercrime Enforcement Act of 2007: Hearing on H.R. 4175 Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 110th Cong. (2007), *available at* http://judiciary.house.gov/Hearings.aspx?ID=192. The witness list consisted of three government officials, a victim of identity theft, the president of a software industry association, and a privacy advocate. *Id.* While many of these witnesses reported statistics about the number of identity theft cases each year, none tried to compare the risks of identity theft with other online or offline risks. *E.g.*, *id.* (statement of Craig Magaw, Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service) (reporting that Secret Service agents had arrested over 4300 suspected identity thieves in fiscal year 2007).

[261] *See infra* Part IV.B.2.b for a description of some academic disciplines attempting

This may be part of a broader trend. Professor Suzanna Sherry has written about a tendency in law and policy to shift away from relying on expert knowledge to consulting mass-created, democratic knowledge.[262] She points to prominent legal scholars in constitutional law, administrative law, and civil procedure who have called for this shift,[263] often in reaction to what they see as the excesses of the power of unelected judges.[264] Sherry is a strong critic of this trend, referring by analogy to two disastrous experiments with the politicization of scientific inquiry: (1) the Soviet Communist party's endorsement of dubious genetic theories known as Lysenkoism and (2) the debate over evolution and creationism in American public schools.[265]

If Sherry is right, then perhaps the devaluation of expertise we see with computers will soon spread to other scientific and engineering disciplines that raise public fears, such as environmental science, genetic engineering, medicine, and biotechnology. Already vulnerable to miscalculated risks, if these fields begin to lose their scientific gatekeepers, the problems of biases and heuristics will worsen and become more difficult to remedy.

3. Self-Interest

Many people are selfishly motivated to portray online actors as sophisticated hackers capable of awesome power.[266] Prosecutors characterize criminal defendants as evil masterminds to gain jury appeal or to enhance a sentence.[267] Law enforcement officials spin

to bring rigor to online risk assessments.

[262] Suzanna Sherry, *Democracy and the Death of Knowledge*, 75 U. CIN. L. REV. 1053, 1053-54 (2007).

[263] *See id.* at 1057 n.10.

[264] *See id.* at 1057 n.9 (citing ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH: THE SUPREME COURT AND THE BAR OF POLITICS 16 (1962)).

[265] *See id.* at 1067-69. Her principal focus is not on scientific expertise, but instead on the "democratization" of legal knowledge, and in particular constitutional interpretation.

[266] Paul Taylor has remarked:

> Despite their diametrically opposed arguments as to the potential social and technical benefits of hacking, both computer security figures and denizens of the computer underground occasionally manipulate and exaggerate the malevolent aspects of hacking (the former to stigmati[z]e and isolate hackers; the latter to revel in the subsequent notoriety such stigmati[z]ation affords).

TAYLOR, *supra* note 29, at xiii.

[267] *See* United States v. Prochner, 417 F.3d 54, 60-62 (1st Cir. 2005) (affirming

yarns about legions of expert hackers to gain new criminal laws, surveillance powers, and resources.[268] The media probably enjoys higher ratings and ad revenue when reporting on online risks.[269] Homeland Security officials specializing in cyberterrorism describe a world full of evil, renegade hackers, bent on terror and destruction.[270] Security vendors do the same.[271]

The DRM debate is unusual, because the self-interest in using the Superuser trope appears on both sides. DRM proponents argue that because they can never win the arms race against powerful users, they need laws like the DMCA.[272] Opponents of DRM argue that the technology is fundamentally futile because all DRM eventually will be circumvented.[273] Because these partisans and litigants have a vested interest in building up the Myth of the Superuser, they obscure the actual reach and influence of Superusers.[274]

application of enhancement because defendant "hacked" into website and rewrote "cgi-scripts"); United States v. Lee, 296 F.3d 792, 799 (9th Cir. 2002) (reversing application of enhancement as applied to designer of fraudulent website); U.S. SENTENCING GUIDELINES MANUAL § 3B1.3 (2000) (requiring two-level adjustment for use of special skill).

[268] *See* Elinor Abreu, *Net Crime Does Pay For Cops*, THE INDUS. STANDARD, Feb. 21, 2000, *available at* http://www.greenspun.com/bboard/q-and-a-fetch-msg.tcl?msg_id=002dvE (citing critics who claim that law enforcement inflates or takes advantage of threat of computer crime to argue for more funding); *supra* Part II.B.

[269] *Cf.* SUNSTEIN, *supra* note 163, at 102-03 (citing increased ratings for cable news stations during reporting about Washington D.C. sniper story of 2002 (citing Johana Neuman, *In a Sniper's Grip: Media's Role in Drama Debated*, L.A. TIMES, Oct. 24, 2002, at 16)).

[270] NATIONAL STRATEGY, *supra* note 86, at 6 (stating that "[b]ecause of the increasing sophistication of computer attack tools, an increasing number of actors are capable of launching nationally significant assaults against our infrastructures and cyberspace").

[271] *See* Levi, *supra* note 22, at 50 (describing "self-serving PR" of "security consultants whose income depends on shocking . . . senior executives and government agencies who complacently fail to spend 'enough' money on security").

[272] *See* Business Software Alliance, Copyright Policy Initiatives to Protect Creative Works: Digital Millennium Copyright Act (DMCA), http://www.bsa.org/country/Public%20Policy/Copyright/Copyright%20Policy%20Initiatives%20to%20Protect%20Creative%20Works.aspx (last visited Apr. 3, 2008) ("The DMCA has helped fuel that expansion by giving software developers and creative artists the tools they need to go after pirates who use technology to steal their products and redistribute them en masse around the world with the click of a button.").

[273] *See supra* Part II.E.

[274] Even those we would not think of as classical advocates or partisans may have a self-interest in inflating the ability of computer criminals. Consider victims, for example. Weak network security is often a contributing factor in the success of a network breach. Victims are unlikely to admit that their security was weak. Low-

4. The Need for Interdisciplinary Work

Finally, too many experts consider online risk assessment to be somebody else's concern. It is not even clear within which field of study the research should occur. Computer security and computer science seem the most likely candidates, because these risk assessments require measuring the rate at which software flaws occur and understanding whether these flaws are easy or difficult to exploit.[275]

Unfortunately, computer security experts often unhelpfully conclude that all computer software is flawed and that malicious attackers can and will exploit those flaws if they are sufficiently motivated.[276] The question is not a technology question at all, they contend, but rather one of means, motive, and opportunity — questions for criminologists and not engineers.[277] Criminologists, for their part, spend little time studying computer crime, perhaps assuming that vulnerability-exploit models can be analyzed only by computer scientists.[278]

Both sides are right and wrong. Assessing an online risk requires both computer science and criminology (as well as economics, psychology, and sociology). Analyses that focus only on some of these disciplines are short-sighted and often flawed.[279]

level administrators responsible for security embellish the sophistication of the attacker to protect their jobs, and their managers do the same thing to minimize liability or bad publicity. Kevin Poulsen, *California Disclosure Law Has National Reach*, SECURITYFOCUS, Jan. 6, 2003, http://www.securityfocus.com/news/1984 (describing "a chronic problem in e-commerce — companies that are hacked are often reluctant to go public for fear of bad publicity or civil liability").

[275] Wade H. Baker, Loren Paul Rees, & Peter S. Tippett, *Necessary Measures: Metric-Driven Information Security Risk Assessment and Decision Making*, 50 COMM. ACM 101, 102 (2007) (describing information security risk assessment as "the product of three main factors: frequency of threats/attacks; the likelihood of their success; and their impact on the organization").

[276] *See supra* note 214.

[277] Email from Author, to Ed Felten, Professor of Computer Science and Policy, Princeton Univ. (Dec. 19, 2006, 09:50:53 MST) (on file with UC Davis Law Review).

[278] For some reason, British criminologists seem much more interested in computer crime, and many have been cited thus far. *See, e.g.*, TAYLOR, *supra* note 29; WALL, *supra* note 22; Levi, *supra* note 22.

[279] *Cf.* Levi, *supra* note 22, at 48 (arguing that problem of computer fraud is "social and internal" rather than "technological and external").

IV. PRESCRIPTIONS FOR MYTH AVOIDANCE

Part III paints a gloomy picture. Fear is a huge problem online. Because it is abetted by the media, compounded by misunderstandings about code malleability, and abandoned by experts, dispelling the Myth of the Superuser is a daunting, difficult task. This Part attempts to rise to the challenge by proposing steps for dealing with the Myth. It is important to recognize that this problem and its solutions are not the same as risk assessment problems encountered elsewhere, such as environmental regulation.

A. Superuser Harm Is Not Global Warming

In *Laws of Fear*, Sunstein ultimately prescribes a kind of "expert cost-benefit analysis" that immunizes policymakers from exaggerated public fears.[280] But because experts have abdicated their role with online harm, the inputs into his proposed cost-benefit analysis — the probability of harm and the level of harm caused by the risk — are very hard to come by.

Sunstein focuses much of his attention on the threat from offsetting harms, and in particular, the harms caused by regulation.[281] For example, mandating expensive measures to reduce global warming emissions may raise the cost of consumer goods, which may increase the levels of poverty.[282] Likewise, Part II demonstrated the grave harms caused by regulations inspired by the Myth of the Superuser.

But despite some similarities, the problems surrounding online harm and computer crime are different from and prior to the concerns voiced by Sunstein. Because the malleability of code inspires new stories and fears as quickly as policymakers can digest them, experts and laypeople view every Superuser as very likely to cause severe harm. This tilts the cost-benefit calculation to justify almost any remedial action, such as increased surveillance powers, harsher penalties, and new restrictions on conduct. The first task, then, is to move from categorical and general pronouncements about Superuser harm to specific data about the likelihood and the severity of online harm.

[280] *See* Dan Kahan et al., *Fear of Democracy: A Cultural Evaluation of Sunstein on Risk*, 119 HARV. L. REV. 1071, 1072 (2006).

[281] SUNSTEIN, *supra* note 163, at 23-34.

[282] *Cf. id.* at 31 (describing how Zambian government's refusal of corn donated from United States due to concerns about genetically modified food could have led to 35,000 deaths by starvation, according to World Health Organization estimates).

B. *Toward a New Empirical Foundation for Online Debates*

I propose a new style of discourse for talking about online conflict. Most importantly, we must demand more extensive and improved quantitative and qualitative empirical evidence. Before we can do that, we need to address the pervasive misuses of anecdote. Storytelling will always be part of our debates, but we must become better producers and more discriminate consumers of the stories that are told.

1. A Moratorium on Suspect Rhetoric

I call for a moratorium on urban myths and just-so stories — tall tales in which the power of the attacks and evasiveness of the attackers increase with each retelling. The earlier discussion of the 1996 Report highlights some of the harmful and pervasive rhetorical tools that are too often used and never challenged.[283] We should ignore, or at least give very little weight to, stories built upon any of the following devices.

a. Mere Possibilities

Logicians describe the "appeal to probability" as the logical fallacy that results when mere possibility is confused with likelihood.[284] Just because something may happen, people conclude that it will happen and that it deserves a response. This is especially troublesome online because the generativity of software seems to makes everything possible.[285]

Bare arguments about what may or could occur should be given almost no weight by policymakers. Given the limits of human bandwidth, most undesirable possibilities will never occur online. Nobody has ever been killed as the result of an online attack.[286] The Internet has never "crashed"[287] and never will.[288] Further, I could find

[283] *See supra* note 19.

[284] *See* Levi, *supra* note 22, at 50 (discussing official sources that "conflate experience of [risk] with theoretical risk from computer crime" (emphasis omitted)).

[285] *See* Zittrain, *supra* note 156 *passim*; *supra* Part III.B.

[286] *See* Krebs, *supra* note 85.

[287] I am unconvinced that the Internet has ever crashed, although, of course, much turns on how I define "crash." In the 2000 Denial of Service attacks that struck Yahoo!, eBay, and others, the vast majority of Internet sites and Internet users continued to operate with little to no noticeable effect. Similarly, although the Morris Worm had a significant effect on a much-smaller Internet in 1988, service was restored in a matter of hours, estimates suggest that only 10% of hosts were infected, and it is almost inconceivable that we would see an outage of similar scale today. *See*

no documented cases of criminals using software booby-traps to destroy evidence.

b. Secondhand Information

Policymakers should be skeptical of the storyteller who is many steps removed from the technical expert or firsthand witness. As children learn from the game of telephone, stories lose important details with each step in the chain. Thus, the longer the chain, the more the story should be doubted.

Furthermore, because the devil is in the technical details, stories of Superuser power should be second-guessed when the speaker lacks the technical knowledge to be trusted with getting the details right. Similarly, stories should be doubted when they have crossed from participant to advocate. All of these problems arise, for example, when stories about powerful computer criminals are reported by legislative affairs officers pressing changes in the laws.[289]

c. Secrecy

Moreover, too many Superuser storytellers enshroud the most important details within veils of secrecy. Security consultants claim the need to protect their clients' identities.[290] Prosecutors refuse to reveal the details of ongoing investigations.[291] The intelligence community refuses to talk about anything.[292]

Paul Graham, The Submarine, http://www.paulgraham.com/submarine.html (last visited Apr. 3, 2008).

[288] *See supra* note 87.

[289] *See* Declan McCullagh, *Porn Spammers to Face Jail in U.S.*, ZDNET.CO.UK, July 9, 2003, http://news.zdnet.co.uk/internet/0,1000000097,2137288,00.htm (quoting Assistant Attorney General William Moschella on Department of Justice's positions on then-pending antispam law); Press Release, U.S. Dep't of Justice, Justice Department Announces William E. Moschella as New Principal Associate Deputy Attorney General (Oct. 2, 2006), *available at* http://www.usdoj.gov/opa/pr/2006/October/06_odag_666.html (reporting Moschella was in charge of DOJ's Office of Legislative Affairs in July 2003).

[290] *See supra* note 253 and accompanying text.

[291] *See, e.g.*, Christopher Hayes, *But Can He Hack Prison?*, CHI. READER, Aug. 19, 2005, *available at* http://www.chicagoreader.com/pdf/050819/050819_cover.pdf. (describing investigation into hack of website and reporting that "[a]n FBI spokesperson says the Bureau won't comment on an ongoing investigation").

[292] *See* Editorial, *The Dangerous Comfort of Secrecy*, N.Y. TIMES, July 12, 2005, at A20 ("The Bush [A]dministration is classifying the documents to be kept from public scrutiny at the rate of 125 a minute.").

In particular, the need to protect victims' rights is a reason why secrecy is given too much deference. For example, corporate victims will often not reveal that their security has been breached.[293] Although such corporations usually claim to worry about customer privacy, they more likely worry about plummeting customer confidence.[294]

While many of these obligations of secrecy are no doubt valid and important, those who labor beneath these restrictions should not be allowed to spin half-stories to influence policy without being required to pierce the veil in return. Stories lacking details, even for legitimate reasons, should not drive policy. I argue that most of the time, they should be given no weight whatsoever.

Also, legislatures should consider laws to eliminate unnecessary secrecy. For example, California now requires companies to publicly disclose security breaches in computer systems that house personal information.[295] Although many companies have criticized this law and opposed similar legislation in other states and in Congress, many privacy and security experts praise the law.[296] Not only does it keep the public better informed about the uses of personal information, but some argue that it provides better data for researchers who want to weigh online risks.[297] As security researcher Adam Shostack explained:

[293] *See* Richard P. Salgado, U.S. Dep't of Justice, *Working with Victims of Computer Network Hacks*, USA BULL., Mar. 2001, *available at* http://www.usdoj.gov/criminal/cybercrime/usamarch2001_6.htm ("Intrusion victims, however, are often even more reluctant to call law enforcement than other business victims.").

[294] *Id.* (reporting that some industry participants in DOJ working group say they did not report past hacks to law enforcement because "the fact of the intrusion will become public knowledge, irreparably shaking investor confidence and driving current and potential customers to competitors who elect not to report intrusions").

[295] *See* CAL. CIV. CODE §§ 1798.29, 1798.82 (West 2002). This is popularly referred to as SB 1386.

[296] *See* Jaikumar Vijayan, *Breach Notification Laws: When Should Companies Tell All?*, COMPUTERWORLD, Mar. 2, 2006, *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,109161,00.html (citing "growing industry consensus that security breach notification laws have forced companies to take more responsibility for the data they own").

[297] Posting of Adam Shostack to Emergent Chaos, http://www.emergentchaos.com/archives/2007/03/security_breaches_are_goo.html (Mar. 29, 2007, 00:43) (describing presentation with slides that can be found at Adam Shostack, Security Breaches Are Good for You (2007), http://www.homeport.org/~adam/Security%20Breaches%20are%20good%20for%20you.pdf). The study of newspaper accounts of security breaches by Erickson and Howard described *supra* note 57, noted a significant increase in reporting since the passage of SB 1386.

> The reason that breaches are so important is that they provide us with an objective and hard to manipulate data set which we can use to look at the world. It's a basis for evidence in computer security. Breaches offer a unique and new opportunity to study what really goes wrong. They allow us to move beyond purely qualitative arguments about how bad things are, or why they are bad, and add quantifatication [sic].[298]

d. Undetectable Power

Because some Superusers' tools are so hard to detect, we will not even know when they have been used. Thus, there is no value pointing to them in policy debates. Consider steganography. A close relative of encryption, steganography involves hiding things in plain view.[299] People use steganographic software to encode messages or files within other files.[300] For example, text messages can be hidden within image files that can then be placed on public websites, remaining hidden in plain view.[301] Although researchers have developed tools to detect some forms of steganography, the research is difficult to conduct and unlikely to be very good at detecting new forms of steganography.[302] Consequently, the spread of steganography is nearly impossible to count or otherwise profile.

The empirical difficulty at the heart of the Myth of the Superuser is at its worst with secret, undetectable tools such as this. Nevertheless, steganography is often cited by scholars trying to (1) justify giving the NSA or FBI more invasive surveillance authority by stating that cunning terrorists are capable of using advanced Internet technology,[303] or (2) prove that new surveillance powers are futile

[298] Shostack, *supra* note 297.

[299] *See* NIELS PROVOS & PETER HONEYMAN, CTR. FOR INFO. TECH. INTEGRATION, DETECTING STEGANOGRAPHIC CONTENT ON THE INTERNET 3 (2001), http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf.

[300] *Id.*

[301] *Id.*

[302] *Cf. id.* (reporting that scan of two million images on eBay had failed to identify any steganographic messages).

[303] *See* Orin Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 607 (2003) (arguing that amending Internet surveillance laws would help War on Terror because terrorists were known to use advanced Internet technologies); Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J. NAT'L SECURITY L. & POL'Y 37, 37 (2005) (explaining that former chief of FBI National

because criminals will simply turn to more secretive ways to communicate.[304] These arguments are supported by journalists who have written articles about how al Qaeda or Osama bin Laden might be using steganography.[305] Thus, because claims about the possible use of Superuser tools like steganography are speculative and inherently irrefutable, they should never be considered effective support in policy debates.

2. Improving the Empirical Foundation: Toward Better Fact-Finding

Ignoring suspect anecdotes will set up the conditions for better policymaking, but this is merely ground-clearing. To truly assess the power of the Superuser, we need better, more reliable, more persuasive facts, and we need to better use the facts we have. Our goal should be to discover whether Superusers or ordinary users account for more harm.

In the course of writing this Article, I had an enlightening email exchange with a technologist at the Electronic Frontier Foundation.[306] He took exception to my hostility to the idea that all DRM is inherently flawed.[307] Early in our exchange, he pointed to the *Darknet* paper as part of his proof of this hypothesis.[308] Although he had not changed my mind (and I do not think I had changed his), by the end of the exchange, instead of relying on a single reference to the *Darknet*

Security Law Unit argued that transactional record information is valuable when hunting terrorists because content information can be obscured, for example, with steganography).

[304] *See* Caspar Bowden, *Closed Circuit Television for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation*, 2002 DUKE L. & TECH. REV. 5, 5 (2002) (arguing against part of then-proposed UK Anti-Terrorism Crime and Security Bill because undetectable communication via steganography would remain undetected).

[305] *See* Jack Kelley, *Terror Groups Hide Behind Web Encryption*, USA TODAY, Feb. 5, 2001, at 7A (citing unnamed "U.S. and foreign officials" for proposition that bin Laden is using steganography); Kevin Maney, *Osama's Messages Could Be Hiding in Plain Sight*, USA TODAY, Dec. 19, 2001, at B6 (acknowledging that "no actual evidence has been found of al[-]Qaeda using" steganography, but engaging in hype nevertheless). The author of the first article, Jack Kelley, was revealed to have made up many of his stories and sources, although the ensuing review of his work did not specifically highlight this article. *See* Blake Morrison, *Ex-USA Today Reporter Faked Major Stories*, USA TODAY, Mar. 19, 2004, at 1A.

[306] *See* Email from Derek Slater, Activism Coordinator, Electronic Frontier Found., to Author (Aug. 15, 2006, 08:50:05 PST) (on file with UC Davis Law Review).

[307] *See id.*

[308] *See id.*

paper, he provided paragraphs of history about the evolution of DRM and DRM crackers and analyses about why DRM is doomed to failure.[309] It occurred to me that this exchange exemplified the result that I seek. Sweeping away the rhetorical shortcut that the Myth of the Superuser represents brings us closer to understanding the true nature of the problems we are trying to solve.

a. Better Using Facts

Before we discover a single new fact, we can make better use of the facts that we have. Even with the moratorium on suspect rhetoric, we cannot abandon anecdotes completely. Because it will be a long time before we gather enough reliable statistics to fully illuminate the risks we face, part of what we must consider will come from stories.

Recall, however, that we are gullible, passive consumers of Superuser anecdotes. To improve, every time we are faced with a Superuser anecdote we should look for competing narratives to help us decide whether the Superuser power or the ordinary user story is the accurate one. For example, despite all of the focus on evil, "black-hat" Superusers, not enough focus is on their counterparts, the "white-hat" Superusers who develop countermeasures. Virus writers are opposed by the antivirus community, spammers battle spam filterers, and system crackers clash with system securers.[310] Policymakers too rarely assess how well white-hat technologists are solving problems on their own. In some of these arms races, the countermeasure community may hold the upper hand, and if we learn to recognize the hallmarks of this arms race, we can learn to wait rather than regulate.[311]

Consider virus writing. The uninformed observer would accept the Myth that powerful, malevolent Superusers create and release damaging viruses and worms and that they do so with impunity. This observer might urge policymakers to expand crimes that punish virus writers. A more informed observer would take into account the following successes of the antivirus community.[312] First, up-to-date

[309] *See id.*

[310] *See, e.g.*, Andrew D. Smith, *McAfee Improves Computer Security, but It's Not Perfect*, DALLAS MORNING NEWS, Oct. 31, 2007, at 1D (interviewing CEO of computer security software firm McAfee).

[311] *See* Ohm, *supra* note 234, at 1984-85 (describing countermeasures designed by Usenet participants and arguing that regulators should consider them when deciding whether to regulate).

[312] Felten's testimony to a House subcommittee inspired this analysis. *See Piracy of Intellectual Property on Peer-to-Peer Networks: Hearing Before the Subcomm. on Courts,*

antivirus software does a pretty good job of preventing the spread of viruses written in the past. Second, computer users who diligently install OS patches and software updates are relatively immune to newly created viruses. Third, only a small percentage of new viruses, particularly those written to exploit new vulnerabilities, will infect the computers of these diligent users. Fourth, only Superusers with significant computer programming ability, plenty of spare time, and access to a community of like-minded attackers, will succeed in infecting these machines; the rest of the would-be virus writers — those with less ability, time, and community — will write duds.

On the other hand, this conclusion perhaps ignores the most relevant observation: many people do not update their virus software and do not diligently install OS patches.[313] Non-Superuser attackers using old tools, some of which are packaged for script kiddies with easy-to-use graphical interfaces, can successfully infect these victims' computers.[314] This goes back to the idea that with viruses, even ordinary users can do great damage.

b. Using Better Facts

Scholars tend to be pessimistic about finding meaningful statistics to measure the basic occurrence of online harm.[315] Perhaps they have not been looking in the right places or asking the right people. There are several promising, rarely tapped groups of researchers attempting to count computer vulnerabilities and exploits.

First, an entire industry for conducting risk assessments of online harm has arisen. Risk assessment theory spans a wide variety of

the Internet, and Intellectual Property of the H. Comm. on the Judiciary, 107th Cong., at 231 (2002) (testimony of Edward W. Felten, Associate Professor of Computer Science, Princeton University), *available at* http://commdocs.house.gov/committees/judiciary/hju81896.000/hju81896_0.HTM. "[A]nalysis of the arms race between virus writers and antivirus companies leads to the prediction that antivirus products will be able to cope almost perfectly with known virus strains but will be largely helpless against novel viruses. This is indeed what we observe." *Id.*

[313] *See* David Talbot, *The Internet Is Broken*, TECH. REV., Dec. 20, 2005, http://www.technologyreview.com/InfoTech/wtr_16055,258,p1.html ("[D]ifferent people use different patches and not everyone updates them religiously; some people don't have any installed.").

[314] *See* Matt Hines, *Unpatched Machines 'Net's Biggest Threat*,' ZDNET.CO.UK, Apr. 26, 2005, http://news.zdnet.co.uk/security/0,1000000189,39196317,00.htm.

[315] *See* Susan Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 VA. J.L. & TECH. 13, *1, n.3 (2004) (noting that there are no "measures and benchmarks for the incidence and damage caused by" computer crime).

quantitative and qualitative methods.[316] The insurance industry, for example, now sells insurance policies relating to computer security.[317] Their studies and the methodologies they employ are rarely cited by policymakers in debates over online threats. This is partly because the industry does not produce the type of detailed analysis that would be most useful for policymakers. Perhaps others can translate the industry's reports to tease out details to make them more useful for policymakers.

A related development is the burgeoning economics of information security discipline.[318] These researchers look at computer and network security as more than just the study of software vulnerabilities, exploits, and countermeasures. They try to account for incentives, externalities, and markets that lead to insecurity.[319]

There are several other pools of untapped statistics about online crime. For example, many organizations monitor online harms for different reasons. Companies that sell virus and spyware scanning software keep statistics about malicious code activity.[320] The Recording Industry Association of America and the Motion Picture Association of America monitor peer-to-peer networks with advanced data-collection "spiders" to track the distribution of their copyrighted works on those networks.[321] More disinterested noncommercial entities such as the SANS Internet Storm Center collect information about threats on the Internet.[322] For example, the Honeynet Project's

[316] *See* CHARLES A. SHONIREGUN, IMPACTS AND RISK ASSESSMENT OF TECHNOLOGY FOR INTERNET SECURITY 68-79 (2005) (describing four quantitative and two qualitative approaches for conducting risk assessments and concluding that none model risk from "technology enhanced information" well).

[317] *But see* Ross Anderson & Tyler Moore, *The Economics of Information Security*, SCI., Oct. 27 2006, at 613 (noting that "the cyber-insurance market is both underdeveloped and underused").

[318] *See generally id.* (providing primer for new economics of information security discipline).

[319] *Id.*

[320] *See* McAfee Avert Labs, Technical White Papers, http://www.mcafee.com/us/threat_center/white_paper.html (last visited Apr. 3, 2008); Sophos, White Papers, http://www.sophos.com/security/whitepapers/ (last visited Apr. 3, 2008); Symantec Security Response, White Papers, http://www.symantec.com/enterprise/security_response/whitepapers.jsp (last visited Apr. 3, 2008).

[321] *See* Benny Evangelista, *Firm Sleuths Out Illegal File Sharers: BayTSP Tracks Down IP Addresses, IDs of Music Downloads*, S.F. CHRON., July 21, 2003, at E1 (describing firm that markets monitoring services of peer-to-peer networks to recording industry copyright owners).

[322] SANS Institute, SANS Internet Storm Center, http://isc.sans.org/ (last visited Apr. 3, 2008).

volunteers set up purposefully vulnerable computers on the Internet to monitor and study computer intrusions.[323] Policymakers and scholars should more aggressively tap into these sources to better profile online threats.

There are no doubt other sources of information and experts in other fields who could contribute to an effort to measure online harm accurately. We should embrace contributions from all of these sources. But bearing in mind the problems of expertise described in Part III.C, we should search for those without vested interests. For example, we should look for those who specialize in fields across an interdisciplinary spectrum with backgrounds in statistics and computer technology.

c. Discovering New Facts

Finally, policymakers should commission new studies to measure the actual incidence of Superuser threats. A good example on the horizon is the ongoing "National Computer Security Survey" cosponsored by the DOJ's Bureau of Justice Statistics and the Department of Homeland Security's National Cyber Security Division and administered by the RAND Corporation.[324] Unlike the CSI/FBI Survey, the latest effort is an ambitious attempt to use rigorous methods to obtain statistically meaningful numbers.[325] According to the survey group, this "is the first and only survey to provide official national statistics on the extent and consequences of computer security incidents within businesses across all industry sectors."[326] Along with other promising methodological choices, the researchers are canvassing businesses in thirty-seven industry sectors, and they plan to repeat the survey every one to two years.[327]

C. The Anti-Precautionary Principle

In *Laws of Fear*, Sunstein critiques the Precautionary Principle, which holds that when faced with evidence of a harm, but uncertainty

[323] The Honeynet Project, Honeynet Project News, http://www.honeynet.org/ (last visited Apr. 3, 2008).

[324] *See* RAND Corp., DOJ/DHS National Computer Security Survey, http://www.ncss.rand.org (last visited Apr. 3, 2008) [hereinafter RAND study website].

[325] For a description of the CSI/FBI Survey and a summary of its criticisms, see *supra* notes 66-74.

[326] RAND study website, *supra* note 324.

[327] RAND study website, *supra* note 324.

about the harm's probability, regulators should act to prevent the harm.[328] Given the historically impoverished empirical evidence that has led to the Myth of the Superuser and the litany of harms that arise when policymakers respond to the Myth, I propose a default — the Anti-Precautionary Principle. In any online conflict, the presumption should be to regulate only the ordinary user unless facts suggest that the Superuser is a significant threat.

Of course, especially given the Myth, there will often be the suggestion that some Superusers exert power. The Anti-Precautionary Principle's presumption will not be invoked. What then? First, if reliable facts establish there are very few Superusers with little aggregate impact, the policymaker should obey the Anti-Precautionary Principle and act as if the Superusers do not exist. That is, when a conflict involves ordinary users in the main and Superusers only at the margins, the harms resulting from regulating the few cannot be justified.

What if the facts point to Superuser domination and significant potential harm? It depends on the strength of that evidence. If the evidence is sound and convincing, the Anti-Precautionary Principle should likely give way, and policymakers should consider regulating the Superuser mindful of the possible harms discussed in Part II.[329] When the evidence is contingent or weak, a pure balancing should apply, comparing the harm caused by the Superusers with the harms caused by regulating.

As an important exception, the Anti-Precautionary Principle should probably yield in the face of horrific potential harms. Policymakers should defer to law enforcement in the face of plausible stories — for example, about terrorist attacks on computer networks that could result in deaths — supported by at least anecdotal evidence that relies on more than the rhetorical devices described in Part IV.B.1.[330] As I

[328] *See* SUNSTEIN, *supra* note 163, at 18-20. Sunstein notes that the Precautionary Principle embodies a range of 20 or more definitions of varying levels of strength. *Id.* at 18. Weak forms of the Principle (noting "lack of decisive evidence of harm should not be a ground for refusing to regulate") are unobjectionable to Sunstein, but it is the strongest forms that he criticizes. *Id.* The form cited in the text is closer to Sunstein's strong forms, and will be the definition used in this Article. Much of what will be said will apply to many different possible definitions.

[329] *See infra* Part IV.D (discussing how to craft minimally harmful laws in this situation).

[330] Sunstein talks about a similar Anti-Catastrophe Principle. SUNSTEIN, *supra* note 163, at 109-15. In the face of an uncertain probability of catastrophe, Sunstein concedes, a form of the Precautionary Principle should apply. *Id.*

suggested earlier, however, experts seem to agree that such attacks are not likely.[331]

To illustrate my proposal, consider the DOJ's recently proposed amendment to § 1030. Under current federal law, causing damage to a computer is a crime only if it causes a sufficient amount or specific type of loss, which for most cases means the victims must have suffered more than $5000 in aggregate losses.[332] There may be fear that the $5000 loss limit will hinder the prosecution of people who deploy and use what are known as "botnets." Whereas traditional computer intruders cause damage or rifle through private files on computers one at a time, a botnet operator collects computers by the hundreds or thousands, causing very little damage to any individual computer.[333] For example, he assembles his "zombie computer army" for future use, ordering them all someday to attack a targeted web server simultaneously.[334] In this situation, during the "quiet collection" phase of the botnet and before the ultimate attack, it would be difficult to show that aggregate harms total $5000.

At a "brown bag lunch hearing" on Capitol Hill,[335] speakers proposed reducing the $5000 threshold.[336] In considering whether to turn this proposal into legislation, Congress should analyze the "Myth of the Botnet General" under my rubric. First, because there have been some confirmed botnet cases, the extent and veracity of this evidence must be scrutinized.[337] The overheated rhetoric will probably suggest that botnets are enormous problems that can cause significant harms, but the evidence made public so far seems predictably unrigorous and largely anecdotal.[338] Ideally, better, more rigorous statistics — perhaps from virus and spyware company studies — could establish the true nature of the risk.

[331] *See supra* note 85.

[332] 18 U.S.C. § 1030(a)(5)(B)(i) (2000).

[333] *See* John Markoff, *Attack of the Zombie Computers Is Growing Threat*, N.Y. TIMES, Jan. 7, 2007, at A1; Press Release, U.S. Dep't of Justice, Computer Virus Broker Arrested for Selling Armies of Infected Computers to Hackers and Spammers (Nov. 3, 2005), http://www.usdoj.gov/criminal/cybercrime/anchetaArrest.htm.

[334] Markoff, *supra* note 333.

[335] Association for Computing Machinery, *USACM Technology Policy Weblog*, Briefing: Learning about the Threats from Botnets (Apr. 20, 2007), http://usacm.acm.org/weblog/index.php?p=490.

[336] *See* Posting of Ed Felten to Freedom to Tinker Blog, http://www.freedom-to-tinker.com/?p=1150 (Apr. 26, 2007, 10:41) (reporting on proposals made by others during hearing).

[337] Markoff, *supra* note 333.

[338] *See id.*

These risks must be balanced against the risks created by getting rid of the $5000 threshold. The threshold serves an important check: it minimizes trivial prosecutions. Many annoying acts occur on networks every day. Spam filters delete nonspam; practical jokes are played in offices on coworkers; files are accidentally deleted from shared servers. Under current law, these non-Superuser acts are not usually prosecuted even though they may fall within the broad and vague conduct elements of the statute's damage prohibitions.[339] Prosecutors and agents who receive a call from a "victim" of one of these acts will almost certainly decline to prosecute or even investigate because they know they will never meet the $5000 loss threshold.

If Congress were to remove the threshold, law enforcement agents could subject harmless people like the office prankster to invasive search and surveillance, and overzealous prosecutors could then bring charges. Given the weak empirical proof about the threat posed by botnets, the risks from removing the threshold outweigh the risks that a botnet owner will someday be apprehended but not prosecutable.[340]

D. Two Additional Difficulties

1. Regulating Actual Superusers

Even if Congress adopts the Anti-Precautionary Principle and begins to demand better empirical evidence, it may conclude that the Superuser threat outweighs the harm from regulating. I am not arguing that Superusers should never be regulated or pursued. But given the checkered history of the search for Superusers — the overbroad laws that have ensnared non-Superuser innocents; the amount of money, time, and effort that could have been used to find many more non-Superuser criminals; and the spotty record of law enforcement successes — the hunt for the Superuser should be narrowed and restricted. Policymakers seeking to regulate the

[339] For example, § 1030(a)(5)(A)(iii) criminalizes access in excess of authorization that causes damage (over $5000) and the subsection has no mens rea requirement. 18 U.S.C. § 1030(a)(5)(A)(iii) (2000). Even unintentional, nonreckless, nonnegligent damage may violate this provision, a misdemeanor for first-time offenders. *Id.*

[340] Given the breadth of substantive federal criminal law, there are almost certainly other federal crimes that could be used to prosecute the Botnet General. *Cf.* Peter J. Henning, *Maybe It Should Just Be Called Federal Fraud: The Changing Nature of the Mail Fraud Statute*, 36 B.C. L. REV. 435, 437 (1995) ("The appeal of the mail fraud statute is its malleability: federal prosecutors can pursue investigations with the knowledge that, in bringing an indictment, they will not be hampered by technical jurisdictional restrictions often found in other federal criminal statutes.").

Superuser can adopt a few strategies to narrowly target Superusers and minimally impact ordinary users.

The chief evil of past efforts to regulate the Superuser has been the inexorable broadening of laws to cover metaphor-busting, impossible-to- predict future acts. To avoid the overbreadth trap, legislators should instead extend elements narrowly, focusing on that which separates the Superuser from the rest of us: his power over technology. They should, for example, write tightly constrained new elements that single out the use of power, or even, the use of unusual power.

Consider, for example, the Superuser-induced phrase, "access without authorization," an element of several different computer crimes.[341] Professor Orin Kerr has noted that courts have construed this vague phrase to apply to many ordinary acts that do not seem to amount to computer hacking, and in many cases, seem unworthy of criminal or even civil sanction.[342] Recall *Explorica*, where a travel agency was found to have engaged in unauthorized access when it scraped information from its competitor's public website, even though it could have used a web browser to obtain the exact same information.[343] In another example, a court held that a man accessed his employer's computer without authorization, which he ordinarily had full permission to access, because he, a faithless employee, sent files to a competitor for whom he planned to work in the near future.[344]

Unhappy with the breadth of these results, Kerr proposed a Superuser-centric amendment. He argued that an act is not done "without authorization" under § 1030 unless the actor circumvented "code-based restrictions on computer privileges."[345] This formulation creates two requirements: first, the computer accessed must have had some sort of "code-based" (i.e., software or hardware based) security or other "restriction[] on computer privileges," and second, the actor had to "circumvent" that restriction.[346] Under this framework, visits

[341] *See* 18 U.S.C. § 1030(a)(1)-(6).

[342] Kerr, *supra* note 103, at 1649-50 (arguing for narrower interpretation of "without authorization" in statute and criticizing cases that have read phrase broadly for "sacrificing a great deal of freedom for a small (and arguably minimal) gain in privacy and security").

[343] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001). Granted, scraping the site with a mere web browser would have been very labor intensive. *Cf. id.* (calling manual alternative "theoretically . . . possible").

[344] Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419, 421 (7th Cir. 2006).

[345] Kerr, *supra* note 103, at 1656.

[346] *Id.*

to public websites would probably not suffice, and breaking an employment contract certainly would not.

As another example, consider again the DMCA, which prohibits the DRM circumvention.[347] One reason the law has been criticized since before its passage is that it places no serious limits on how sophisticated a lock must be before it gains the backing of the prohibition.[348] Although the law extends only to DRM that "effectively controls access" to a copyright-protected work, that phrase is defined to mean that the DRM "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."[349] Courts have interpreted this to place almost no restrictions on the level of sophistication required — even DRM that is trivial to unscramble will satisfy the low hurdle for protection.[350]

The DMCA can be rewritten to focus more specifically on the Superuser while not casting its overbroad net on ordinary users. For example, "effectively controls access" could be amended to apply only to digital locks that pass a particular threshold of complexity. Perhaps this could be defined in terms of encryption algorithms that have been sufficiently peer-reviewed or by uses of a 128-bit symmetric key length.[351] Perhaps a regulatory process can define the level of technology protected.

The point is to try to create a balance between addressing the harm — indiscriminate cracking of DRM and rampant copyright infringement — and ensuring that average, ordinary users are not prosecuted for doing ordinary things or investigated for months before

[347] 17 U.S.C. § 1201(a)(1)(A) (2000).

[348] *See* Cohen, *supra* note 34, at 172-73.

[349] 17 U.S.C. § 1201(a)(3)(B).

[350] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000) ("Finally, the interpretation of the phrase 'effectively controls access' offered by defendants at trial-viz., that the use of the word 'effectively' means that the statute protects only successful or efficacious technological means of controlling access — would gut the statute if it were adopted.").

[351] Holding everything else constant, the longer (the more bits) the key used, the harder it is (the more computation time it requires) to crack encrypted ciphertext. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 152 (2d ed. 1996) ("Two parameters determine the speed of a brute-force attack: the number of keys to be tested and the speed of each test."). Although the details are well outside the scope of this Article, cryptographic algorithms come in two broad flavors, public-key and symmetric-key cryptography. For any given key length, it is easier to crack a public key than a symmetric key. *Id.* at 166 tbl.7.9. A 128-bit key length is still somewhat respectable for a symmetric key algorithm, but it is laughable for public key cryptography. *Id.*

the pall of suspicion passes over them.[352] In short, the idea is to craft laws that are tailored to the type of power that Superusers wield.[353]

2. Regulating Prometheus: The Problem of Script Kiddies

Finally, sometimes Superusers empower ordinary users with easy-to-use software.[354] These "script kiddies," as they are known in computer security jargon, are like modern Prometheuses given great power from above. How does this threat fit within a model that urges inattention to Superusers?

First, the script kiddie should be part of the cost-benefit accounting. When policymakers are balancing competing harms, they should factor in the possibility that Superusers will empower legions of ordinary users. As always, bare assertions that this kind of empowerment is likely or inevitable should be met with suspicion. After all, there is probably a "Myth of the Script Kiddie."

Second, and more controversially, there are steps to keep Superusers and script kiddies apart. Professor Randy Picker has proposed what he terms an "incentive wedge" to keep honest, ordinary users from using DRM circumvention tools.[355] Specifically, he proposes embedding digital music and movies with personally identifiable information that can direct future investigators back to the source.[356]

[352] *See* Electronic Frontier Foundation, US v. ElcomSoft & Sklyarov *FAQ* (Feb. 19, 2002), http://www.eff.org/IP/DMCA/US_v_Elcomsoft/us_v_sklyarov_faq.html (describing indictment of Dmitri Sklyarov for circumventing some very weak protection schemes of DRM on Adobe eBook reader).

[353] The obvious downside to this proposal is that defining criminal acts with respect to technical power can lead to the guilt by association problem described above. If lawmakers create prohibitions defined by a person's technical sophistication and power, other elements of those prohibitions must protect researchers, students, security professionals, and others, who act powerfully but without evil intent or harm. For example, the harm elements of the prohibition should be definite and clear, so that a researcher who circumvents DRM but does not create downstream copies or release automated tools will not be covered.

[354] *See* Erickson & Howard, *supra* note 57, at 12 ("Since knowledge and tools developed by more experienced hackers can easily be obtained on the Internet, the capability to penetrate insecure networks has propagated outside of the legitimate hacker community to other groups, ranging from inexperienced teenagers to international crime syndicates.").

[355] Picker, *supra* note 33, at 49.

[356] *Id.* at 69. Ed Felten disagrees. Posting of Ed Felten to Freedom to Tinker Blog, http://www.freedom-to-tinker.com/?p=980 (Feb. 22, 2006, 13:54) (calling Picker's idea "an instructive idea, but not a practical one"). Apple Computer began embedding the names of customers into the songs they purchased through iTunes. May Wong, *Questions Raised over iTunes User Data*, USA TODAY, June 5, 2007, *available at*

Even more controversially, faced with a conflict in which Superusers have not yet empowered script kiddies, perhaps Congress should ban the creation or distribution of script kiddie empowering tools. This idea gives me significant pause because of Congress's checkered track record at drafting this kind of regulation, but some lessons can be learned by looking at past attempts. The DMCA, which prohibits the creation and distribution of DRM circumvention tools,[357] and § 2512 of the Wiretap Act, which prohibits the creation and distribution of particular types of wiretapping devices,[358] are two prominent examples of laws that prohibit the distribution of software. Comparing these two laws raises an interesting question. Why is the DMCA's distribution prohibition so controversial while § 2512 is not? The answer may serve as a map for creating less controversial software distribution bans.

There are some obvious possibilities. First, § 2512 is very rarely prosecuted.[359] Although the DMCA also rarely leads to criminal charges, it is often rattled like a saber by civil litigants.[360] Second, § 2512 predated the spread of the Internet and the rise of online civil liberties groups.[361] If § 2512 were proposed anew today, it would almost certainly meet fierce opposition.

There is a less intuitive, more intriguing possibility: the DMCA targets technology that has potentially beneficial, legal uses. Many law-abiding citizens would like to circumvent DRM to backup their

http://www.usatoday.com/tech/products/services/2007-06-05-itunes-drm-free_N.htm.

[357] 17 U.S.C. § 1201(a)(2) (2000).

[358] 18 U.S.C. § 2512 (2000).

[359] A search of Westlaw's ALLFEDS database for the phrase "18 U.S.C. § 2512" on February 6, 2008 returned 19 cases. Almost all of these cases were civil lawsuits brought by DirectTV seeking to use the provision against people selling and buying satellite TV descrambler chips. *See, e.g.*, DirectTV, Inc. v. Barnes, 302 F. Supp. 2d 774 (W.D. Mich. 2004). The search returned four criminal prosecutions. United States v. Biro, 143 F.3d 1421, 1422 (11th Cir. 1998); United States v. Daniels, 978 F.2d 415, 416 (8th Cir. 1992); United States v. Novel, 444 F.2d 114, 114 (9th Cir. 1971); United States v. Spy Factory, Inc., 951 F. Supp. 450, 451-52 (S.D.N.Y. 1997).

[360] *See* Chilling Effects Clearinghouse, http://www.chillingeffects.org (last visited Apr. 3, 2008) (collecting and displaying copyright-related cease and desist letters).

[361] A form of § 2512 was part of the original Wiretap Act enacted in 1968. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §802, 82 Stat. 214. In comparison, the EFF was founded in 1990, EFF, About EFF, http://www.eff.org/about (last visited Apr. 3); the Center for Democracy and Technology in 1994, CDT, Summary of CDT Activities 2000 — Work Plan 2001, http://www.cdt.org/mission/activities2001.shtml (last visited Apr. 3, 2008); and the Electronic Privacy Information Center also in 1994, EPIC, About Epic, http://epic.org/epic/about.html (last visited Apr. 3, 2008).

movies and software, time-and-space shift television,[362] or practice other fair uses.[363]

There are fewer reasons why the general public needs tools that are "primarily useful for the surreptitious interception of communications" — the tools prohibited under § 2512.[364] People in messy divorces and whistleblowers may need to surreptitiously record audio conversations, and network systems administrators and concerned parents may need to monitor computer communications, but these people can use general purpose tools — tiny voice records and network packet sniffers — that do not fall within the prohibition. Unlike the DMCA, § 2512 seems narrowly targeted at devices like transmitters hidden in calculators[365] and specific forms of spyware.[366]

If regulators are bent on keeping Superusers and script kiddies apart, perhaps they should try to model laws after § 2512 rather than the DMCA. If one characteristic of a tool is especially pernicious and unlikely to be useful for widespread, legitimate use, a narrow law can be written criminalizing the creation or distribution of that tool.

CONCLUSION

Fear is with us for the long haul. With any technology as complex and as relied upon for so many different commercially important uses as the Internet, some will exploit disparities in knowledge to gain power to harm others, sparking uncertainty and fear. Opportunists will take advantage of this fear for personal and institutional gain. To date, the fear mongers have had the upper hand, shaping policy through sound bites and unfounded anecdotes.

Even if unchecked, the fear mongers will not spell the end of the Internet. I am not predicting an information apocalypse. But if they continue their stranglehold on policymaking debates, they will eventually shape the future Internet. Policymakers will impose new

[362] *See generally* Sony Corp. v. Universal City Studios, 464 U.S. 417 (1984) (discussing time shifting); Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072 (9th Cir. 1999) (discussing space shifting).

[363] 17 U.S.C. § 107 (2000); *see* Cohen, *supra* note 34, at 177.

[364] 18 U.S.C. § 2512 (2000).

[365] *See* United States v. Biro, 143 F.3d 1421, 1423 (11th Cir. 1998) (affirming convictions under § 2512 for sale of transmitters hidden in wall plugs, pens, and calculators).

[366] *See* Press Release, U.S. Dep't of Justice, Creator and Four Users of LoverSpy Spyware Program Indicted (Aug. 26, 2005), http://www.usdoj.gov/criminal/cybercrime/perezIndict.htm (announcing indictment relating to spyware designed to masquerade as e-greeting card).

regulations to constrain conduct and chill expression. Witness the steady expansion of the CFAA. Technologists will create next generation technologies ostensibly designed to protect, but also designed to monitor and control. Consider how improvements in virus-blocking firewall technology can be used by repressive governments to search for dissident speech. Given another decade to drive policy, the fear mongers will not destroy the Internet, but they will change it for the worse.

Of course, fear mongers exist outside this narrow viewscreen; thus, in some ways, theirs is not the interesting story here. The truly troubling problem lies with the experts who have abdicated their responsibility to discover facts and assess probabilities of risk. Experts can reclaim some rhetorical space from the fear mongers, but to do so they will need a rigorous, focused, interdisciplinary approach.

I worry that the abdication of expertise is a canary in a coal mine, alerting us to a broader, evolving failure of expertise in our society. As the definition of expertise broadens and democratizes, the effects of fear are compounded and the biases and heuristics they introduce become more difficult to identify and intractable to root out. In a world without experts, or where everyone is an expert, we will look back on today's teeth-gnashing over how laypeople ignore expert predictions about, for example, global warming with wistful nostalgia.

This bleak prediction is but one path we can take. By exposing the ubiquity and persistence of online fear, and by prescribing the medicine needed to regulate intelligently in the face of fear, this Article points the way toward a restoration of expertise, and a move to principled, cautious, justified policymaking and debate.