

THE MYTH OF THE SUPERUSER

Paul Ohm^{*}

ABSTRACT

Most Internet users are relatively unsophisticated, exercising limited power and finding themselves restricted by technological constraints. Other users, the minority, have great power and can bypass such constraints. The user with power—the “Superuser”—is the subject of this Article. He (always he) is a mythic figure who circumvents DRM, moves from Internet host to host anonymously, knows every zero-day vulnerability, and writes his own exploits. He is difficult to find, expensive to catch, and aware of every legal loophole. He terrifies lawmakers. Regrettably, concern about the Superuser has led to confusing and ambiguous laws and has been used to justify infringements on individual rights such as the privacy of online communications. Severe costs like these are unwarranted because the Superuser is simply not very important in many online conflicts.

In this Article, Paul Ohm argues that too much attention is being paid to the Superuser. For most online conflicts, the Superuser likely plays a very small role.

ABSTRACT	1
INTRODUCTION	2
I: THE SUPERUSER	4
A. STORYTELLING	4
B. THE SUPERUSER DEFINED	5
C. THE SUPERUSER AND ONLINE CONFLICT	6
D. WHY THERE WILL ALWAYS BE SUPERUSERS	7
II. THE MYTH	9
A. THE MYTH DEFINED	9
B. EXAMPLES OF THE MYTH IN ACTION	9
1. <i>The Computer Fraud and Abuse Act</i>	9
2. <i>Scholars and the Myth: Steganography and IP Spoofing</i>	11
C. REASONS FOR THE MYTH	13
1. <i>Reason One: Self-Interest</i>	13
2. <i>Reason Two: The Media</i>	14
3. <i>Reason Three: Technological Ignorance and Fear</i>	15
D. THE SUPERUSER IN THE NON-COMPUTER WORLD	16

* Associate Professor, University of Colorado School of Law. I previously served as a Trial Attorney in the Computer Crime and Intellectual Property Section of the U.S. Department of Justice. In this position, I advised federal prosecutors about some of the criminal cases cited in this article. Everything I say about these cases is based on the public record, and nothing I say should be construed to be the view of the Department of Justice. I will not specifically highlight my participation in the cases cited.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

III. THE PROBLEM WITH THE MYTH.....	17
A. WHAT IS WRONG WITH BELIEVING IN THE MYTH?	17
1. <i>The Hasty Generalization</i>	17
2. <i>Metaphor Failure</i>	19
3. <i>Guilt by Association</i>	20
4. <i>Misallocated Resources: Superusers are Hard to Find and Stop</i>	20
B. THE EFFECT OF THE MYTH ON LEGISLATION	21
1. <i>Overbreadth</i>	21
2. <i>Types of Criminal Elements: Conduct, Results, Intent, Attendant Circumstances</i>	21
3. <i>The Investigatory Funnel</i>	22
C. THE EFFECT OF THE MYTH ON JUDGES	26
1. <i>Judges and the Myth</i>	26
2. <i>Example: Search Warrants for Computers</i>	26
D. THE EFFECT OF THE MYTH ON SCHOLARS	28
IV. PRESCRIPTIONS, ADDITIONAL DIFFICULTIES, AND FUTURE WORK	32
A. PRESCRIPTIONS	32
1. <i>The Facts Behind the Myth</i>	32
2. <i>Advice for Lawmakers, Judges, and Scholars</i>	35
3. <i>60/40, 80/20, or 99/1?</i>	38
B. ADDITIONAL DIFFICULTIES	39
1. <i>Script Kiddism</i>	39
2. <i>Dealing with Actual Superusers</i>	43
CONCLUSION.....	47

INTRODUCTION

Most Internet users are relatively unsophisticated, exercising limited power and finding themselves restricted by technological constraints. Other users, the minority, have great power and can bypass such constraints. The user with power—the “Superuser”—is the subject of this Article. He (always he) is a mythic figure who circumvents DRM, moves from Internet host to host anonymously, knows every zero-day vulnerability, and writes his own exploits. He is difficult to find, expensive to catch, and aware of every legal loophole. He terrifies lawmakers. Regrettably, concern about the Superuser has led to confusing and ambiguous laws and has been used to justify infringements on individual rights such as the privacy of online communications. Severe costs like these are unwarranted because the Superuser is simply not very important in many online conflicts.

In this Article, I argue that too much attention is being paid to the Superuser. For most online conflicts, the Superuser likely plays a very small role. I develop this general point by focusing on three specific conflicts: digital rights management, unauthorized access to computers, and the search and surveillance of computers and networks. I revisit these battlegrounds throughout the Article to demonstrate how the rhetoric of the Superuser has cut off otherwise useful ideas and debate. This is so despite the absence of empirical proof that these battlegrounds are overrun by Superusers and despite the presence of some evidence to the contrary.

I focus in particular on criminal prohibitions and criminal procedure. What form do criminal laws take when written to combat the Superuser? How do the laws governing

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

search and seizure evolve in response to the threat of the Superuser? Although I spend less time looking at other types of regulations such as tort and contract law, much of what I conclude applies to those areas as well.

Lawmakers respond to the specter of the Superuser by drafting laws that are vague and broad. Law enforcement officials and civil plaintiffs bring cases that use these vague, broad laws to sweep in innocent people who were not the original targets of the laws. Judges sow confusion into common law doctrines that turn on reasonableness or the ordinary observer by envisioning a world full of Superusers.

Meanwhile, the Superuser is the white whale of Internet scholarship, often discussed but only as a caricature and never fully theorized. To legal scholars, he disrupts expectations because his actions defy analogy and metaphor. If you place a virtual “wall” in front of him he can walk through it or fly over it. Overly mindful of this disruptive power, scholars dismiss their own or others’ creative solutions.

I define the Superuser in Part I and the Myth of the Superuser in Part II, and for both, I look for root causes. In Part III, I argue that the Myth of the Superuser has been harmful to privacy, efficient and effective law enforcement, and sensible Internet regulation. I explain how lawmakers, judges, and scholars have brought about these harms in related but distinct ways.

In Part IV, I offer a number of prescriptions for lawmakers, judges, and scholars to address the Myth. Foremost, new methods for and better efforts at counting Superusers must be undertaken. Additionally, Lawmakers should usually legislate as if the Superuser does not exist. Prohibitions should be narrowly tailored to capture actual bad acts, instead of written broadly to “adapt” to tomorrow’s Superuser-instigated new harms. Judges should measure “reasonableness” and “expectations” online from the vantage point of the ordinary user. Scholars should not allow the hypothetical presence of the Superuser to scuttle otherwise-workable solutions.

Finally, ignoring the Superuser raises some new difficulties that I address, also in Part IV. First, I consider “script-kiddism,” the term for the Superuser empowerment of average users through easy-to-use tools. Although the risk of this can be overblown, it is a genuine problem, and I propose methods for keeping Superusers and script kiddies apart. Second, ignoring Superusers is not always possible or wise, because some Superusers cause significant harm. For these cases, I urge the creation of targeted laws that are likely to ensnare the Superuser but not the ordinary user.

In this article, I challenge a rarely challenged, troublesome rhetorical device that’s built upon difficult-to-rebut empirical facts. I doubt that this article will end the use of the Myth of the Superuser, once and for all, but I hope at least to call its more troubling uses into question.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

I: THE SUPERUSER

A. Storytelling

As this is an argument about storytelling and rhetoric, let's begin with three brief stories:

- In the early-1990's, a juvenile gained access to a computer in Worcester, Massachusetts, that controlled an important telephone switch. At some point the juvenile reset the switch, disabling local phone service in the area.¹ This particular switch happened to carry phone communications for the local, small, unmanned airport, and by disabling the switch, the juvenile made it impossible for incoming aircraft to turn on the landing lights. No planes crashed, and nobody was injured, but the story continues to resonate. Replace the juvenile with international terrorists, the small regional airport with O'Hare, and the inadvertent effect with an intentional attack, and the lesson is unmistakable.²

- Apple's iTunes music store sells songs that have been protected by a "digital lock" using digital rights management technology (DRM) called "FairPlay." FairPlay lets purchasers listen to their music in "authorized" ways on "authorized" computers, but attempts to prevent unauthorized uses and copies. Norwegian programmer Jon Johanssen developed several software programs that could strip the protection from a FairPlay protected song, albeit only by the legitimate purchaser of a song or by someone with access to the purchaser's password. Other programmers have written similar software targeted at iTunes protected music.

- [Booby-Trapped Computer Story.]

The common thread between these three stories is they feature the power of computer users. The three people in these stories each did something with a computer that most people would not know how to begin to do. Digging deeper, these are all stories about online struggles between competing factions, and at least one faction in every story considers the power described a threatening harm. Legislators, among others, worry about the airport hacker; content owners fear the DRM circumventor; and law enforcement agents are concerned about the evidence destroyer.

These stories and this kind of storytelling could be useful to the debates that take place about these conflicts—computer crime, DRM, and computer search and seizure law—if they were cited for what they were: interesting anecdotes that may provide a window into the empirical realities of online conflict. Instead, stories like these subsume the debate, and are wielded by partisans as replacements for a more meaningful empirical inquiry. The prevailing 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

¹ Scott Charney, *Transition Between Law Enforcement and National Defense* contained in SECURITY IN THE INFORMATION AGE: NEW CHALLENGES, NEW STRATEGIES, Joint Economic Committee, U.S. Congress (May 2002) available at www.house.gov/jec/security.pdf.

² See *id.*

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

kill airline passengers; DRM is inherently flawed; and computer criminals booby-trap their computers to self-destruct.

Storytelling about power-users is epidemic in online disputes. These stories are used as soundbites that replace more productive, more factually grounded debate. The reasons for this are many, and the remedies are not hard to achieve, but let us first define some terms.

B. The Superuser Defined

A Superuser is a computer user who can effect change (both with and without authorization) to computers or networks that ordinary users cannot.³ Power—the ability to effect change—is necessary but not sufficient to be a Superuser. Merely ordinary users can effect great change if they use the right software, but this power does not make them Superusers. Consider this example: in the late Nineties, users could browse the music collections of millions of other people and copy songs from any of them in minutes using Napster, yet those users were not acting as Superusers, as I have defined it. They wielded great power, but because the power came from easy-to-use software used by millions of people, they were not Superusers. The term is a relative one.

Why do Superusers exist? Superusers tend to have more (1) time; (2) practice; (3) access to tools; or (4) knowledge about computer technology and networks than ordinary users. Often, Superusers have more than one of these, but they need not have all of them. The four sometimes feed one another, as more time can be used to practice and more practice can be used to gain knowledge. These attributes develop Superuser power, and no innate traits are required.⁴ Many ordinary users could become Superusers, if only they had the time, practice, tools, or knowledge to do so.

Not only is Superuser a relative term, it is a temporal term. People with the power to do X may be considered Superusers today and ordinary users six months from now. A person is a Superuser only so long as the fraction of users with his power is small. When a critical mass of other users gains the ability to do what only a Superuser once could do, the label disappears.

Take the example of audio CD ripping. Not too long ago, when the audio CD format was new and CD-ROM drives were scarce, few people could do what is now known as ripping: copy the bits off of an audio CD onto a computer into a playable file format (such as wav or mp3). These people were Superusers. Soon thereafter, some of them

³ In the various flavors of UNIX and UNIX-like Operating Systems, “superuser” (lowercase ‘s’) is the name given to the user account that can be used by a system administrator to make almost any change to the system. *See* Kaare Christian and Susan Richter, *THE UNIX OPERATING SYSTEM 65* (Wiley 1993). Typically, the superuser does not act maliciously and is authorized to do what he or she does. According to my definition, every superuser is a Superuser, but every Superuser is not a superuser. I use capitalization to distinguish between the two.

⁴ Intelligence does not separate the average Superuser from the ordinary user—there are stupid Superusers and bright ordinary users—although intelligence doesn’t hurt.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

packaged the ability to rip CDs in functional but not necessarily polished computer programs. Thanks to these tools, the percentage of people with the CD ripping power increased, perhaps substantially. Depending on how much that percentage had changed, the software-empowered rippers may or may not have become Superusers, under my definition.⁵

Today, the ability to rip a CD, while probably still not a skill exercised even by the computer user of median ability (however that is defined), is no longer a Superuser skill. Ripping software has changed in two critical ways to bring about this shift. First, the software has become easier to use, as the functional, unpolished programs of five years ago have become polished, intuitive tools. Second, the software has become easier to obtain. Windows XP, Mac OS X, and iTunes all come bundled with the software required to rip CDs.⁶

This example highlights the importance of tools: very often, whether or not a task is restricted to Superusers depends completely on the ease-of-use and availability of software. A corollary is the phenomenon known as “script kiddism.” “Script kiddies” are ordinary users who can perform tasks that were previously performable only by Superusers, because the users have been empowered by easy-to-use tools. I will discuss the script kiddie’s effect on the Myth of the Superuser in Part IV.B.1.

C. The Superuser and Online Conflict

The Superuser is regularly featured in debates about online conflict. Using his power, he can disrupt almost any battle between Internet combatants. Here are some examples that will be revisited through this article:

Music/Movie Piracy and DRM: Digital Rights Management (“DRM”) technologies make it difficult to copy or otherwise access computer files, such as movies or music. DRM gives technical teeth to copyright law’s prohibitions against the making of unauthorized,

⁵ Even if they weren’t technically “Superusers,” these people no doubt would still have seemed extraordinary to ordinary users.

⁶ There are countless other examples. Take 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 ftp protocol, write (without the assistance of any specialized tools) a web page containing those photos, and then e-mail the URL to your friends and relatives. A little less than a decade ago, you could use a 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 much more polished results.

One more: To send anonymous e-mail in the early 1990’s, you had to issue a series of precise commands (which complied with the SMTP e-mail protocol) to an e-mail server. In the late 1990’s, anonymous remailers were set up in foreign countries that would strip identifying information from incoming messages and forward them onto their destination. Today, setting up an account at Yahoo! or Gmail is a quick way to be able to send pseudonymous e-mail messages.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

non-fair use copies. A fierce debate over DRM rages. The debate often focuses on whether the force of law should be given to DRM locks, by making it illegal to circumvent DRM (i.e. pick the locks) or to teach others to do the same.

The Superuser helps frame this conflict. Superusers know how to pick locks that ordinary users do not. While computer science theory suggests that all digital locks can eventually be picked,⁷ some locks are trivial to pick, even by the ordinary user. Other locks can be picked by many, with the help of easy-to-use and readily-available tools. Finally, the strongest locks can be broken only by a small number of Superusers.

Computer Security and Unauthorized Access: Access to computers on the Internet is restricted by software and hardware-based security systems. These systems are quite complex, and each day brings news of the discovery of new flaws in them that can be exploited—usually by Superusers—to circumvent computer security to gain unauthorized access. Ordinary users, even if they desire to break into a particular computer, usually lack the time, practice, tools, or knowledge to do so.

Surveillance: Government data finders battle against criminal data hidiers. The two sides are said to use Superuser tactics, respectively to uncover and to hide communications. The government's law enforcement officers and intelligence agents try to acquire and sift through large volumes of data stored on computer hard drives and in transit through computer networks, in search of evidence of crime or threats to national security. If the world were full of ordinary users, the government would usually find the evidence it sought. Instead, Superuser data hidiers obscure their actions with creative and evolving techniques.

The common element of these stories is the Superuser: a disruptive force who can tip these battlefields to his favor. The common missing element in these stories is a measure of the prevalence of the Superuser. If only a tiny percentage of users can act as a Superuser, they may not realistically pose the risk of disruptions suggested above. If, on the other hand, Superusers are many, are possessed of significant disruptive power, and are working to empower ordinary users to follow their lead, the battlefield is probably now or will soon be tilted significantly in their favor.

D. Why There Will Always be Superusers

Why are Superusers a persistent presence in online conflicts? Why can't programmers simply create more robust software? Superusers exist because of several well-known features of code, computers, and networks that are unlikely to change in the near future: First, sometimes Superusers are intentionally empowered. Second, computer software and hardware are designed to be open, malleable, and in many instances, in the physical possession of the end user. Similarly, computer networks are open and dynamic. Finally, it is impossible to write perfect, bug-free software.

⁷ [CS Literature]; [Felten blog posts.] This is a weaker claim than saying that all locks *will be* broken. Many scholars have confused the weaker claim for the stronger. See Part III.D.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

Some Superusers are intentionally empowered to do what they do. Software programmers are often themselves Superusers, and they understand and appreciate why someone would want to use their software in a more efficient way. “Expert level access” is often built into software. Consider, for example, the Windows Command Prompt and UNIX shell. With these text-only programs (which are quite homely by today’s graphical standards) users enter esoteric commands to copy files, create folders or run programs. Much of what can be done with these programs can be done more intuitively using a graphical program such as Windows Explorer. Why do some users insist on using these programs instead? First, people who are experts with the Command Prompt or shell are often more efficient than their graphical interface-using counterparts. Second, some things can be done “at the prompt” that are impossible with a graphical program.⁸

Superusers also thrive in today’s computer networks due to the inherent openness of software and hardware design.⁹ Computer hardware is usually shipped with an easy-to-open plastic case that invites tinkering, even though most computer users will never tinker. Computer software is shipped in a metaphorically similar manner, with the typical Operating System, for example, shipped to allow “administrator access” by the average user.

These design choices are not mandatory. Hardware could be shipped sealed and inaccessible. The OS could allow only limited control. If those choices were the status quo, it would be more difficult to be a Superuser. This is why experts modify and adapt the open PC much more easily and often than the closed, hard-to-modify TiVo.¹⁰

Networks are also intrinsically open. Good thing, too, because openness is a primary reason why the Internet has grown so rapidly to include so many exciting and innovative services. Superusers have taken advantage of this openness, too.

Further, those who designed the Internet built a large amount of trust into it. So, for example, robust authentication—mechanisms to verify that a person communicating online is who they say they are—is not built into the Internet. Authentication has been “bolted on” in some cases, but the unauthenticated core always lurks beneath. Superusers take advantage of built-in trust to do what was not intended and to do so undetected.

The final, and significant, reason why we will always have Superusers is because software will always be imperfect. All software programs, which are more complex than the truly trivial, have bugs.¹¹ Bugs exist because it would be too expensive to drive them all away. At some point, the cost of finding the next bug will outweigh the odds that the next bug will cause significant harm or that anybody will find the bug at all. Superusers

⁸ The reverse is also true.

⁹ See Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1982-87 (2006).

¹⁰ See *id.* at 2014-15.

¹¹ [CS Literature.]

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

find and exploit bugs to circumvent security, break DRM, or otherwise cause software to do what it is not designed to do.

II. THE MYTH

A. The Myth Defined

The Myth of the Superuser is the belief that to resolve an online conflict, one must find a way to deal with Superusers who can circumvent technical restrictions and evade detection and identification. The Myth is flawed, as I will explore more fully in Part III, because Superusers are often so uncommon as to be inconsequential. Even when Superusers *can* flout or circumvent a conflict's solutions, if these solutions can yet constrain the ordinary users, they are good enough.

Put more generally, the Myth is any reference to Superusers to support or oppose a proposal to resolve online conflicts. Proponents of laws invoke the Myth when they urge legislation to deal with the "growing problem of hackers." Lawmakers fall prey to the Myth when they pass broad laws designed to punish Superuser-criminals. Scholars sidestep important issues by raising the Superuser to bolster arguments or refute others' arguments.

B. Examples of the Myth in Action

1. The Computer Fraud and Abuse Act

Congress in particular tends to fall prey to the Myth. The Computer Fraud and Abuse Act—the principal Federal law that criminalizes computer hacking and trespass—and in particular section 1030 of Title 18 exemplifies the trend. Although criminal cases and civil lawsuits are brought under this section only a few times per year,¹² Congress has overhauled it at least five times since adopting it in 1984.¹³ Many of these changes have broadened the scope and terms of the prohibition and have been justified by lawmakers and law enforcement officials as ways to deal with the perceived threat of the Superuser.

Consider, for example, the amendments made to the statute in 1996 in the National Information Infrastructure Protection Act of 1996.¹⁴ [The Senate Judiciary Committee held hearings¹⁵ at which Attorney General Janet Reno, FBI Director Louis Freeh, and the U.S. Secret Service Deputy Assistant Director testified. [More on hearing.]]

The Senate Report confirms that the Committee accepted the Myth of the Superuser. The report is replete with anecdotes about nefarious and powerful hackers who might not have been covered by the then-existing version of section 1030. "Hackers," we are told,

¹² See Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 *Hast. L. J.* 805, xx (2003).

¹³ [String cite of amendments.]

¹⁴ Pub. L. 104-294, Title II, s 201 (1996). (Passed as Title II of the Economic Espionage Act).

¹⁵ Get cite for 10/30/95 and 2/28/96 Hearings (also House Banking hearings of 10/11/95.)

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

“have broken into Cray supercomputers for the purpose of running password cracking programs, sometimes amassing computer time worth far more than \$5,000.”¹⁶ The hackers are anonymous, the incidents are too, and we are never told whether these mythical Superhackers were caught, and if so, whether Federal charges could not be brought against them because of gaps in the statute.

Later in the report, to justify a broadening of the prohibition of a subsection of 1030, the Committee reported that “intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later.”¹⁷ Again, the report provides no other details about these incidents.

The parade of horrors reaches its high point with the Committee's justification for an entirely new prohibition, section 1030(a)(7). Although in 1996, extortion was already a Federal crime that had been on the books for decades, the Committee created an entirely new prohibition criminalizing “a new and emerging problem of computer-age blackmail.”¹⁸ Evidently, the world had been plagued by the scourge of people making threats against computer systems. Ignoring the fact that a threat against a computer system is no less extortionate than a threat against a person and thus covered by the pre-existing law, the Committee proposed (and ultimately Congress adopted) a new crime that borders on the cartoonish: “make one false move and the ThinkPad gets it!”

To justify this seemingly unnecessary new law, the Committee used some of its worst Superuser rhetoric. First, they passed the buck. “According to the Department of Justice, threats have been made against computer systems in several instances.”¹⁹ The Committee also engaged in hypothetical musing. “One can imagine situations in which hackers penetrate a system, encrypt a database and then demand money for the decoding key.”²⁰ Nowhere in the record are specific examples of when this law would have helped prosecute someone who otherwise had fallen outside the statute.

The result is a law that is almost a dead letter. In the decade that it has been on the books, 1030(a)(7) has been cited in the Federal Reporters twice. One case involved an honest-to-goodness extortionate threat made by Russian hackers,²¹ the other involved a spurious civil claim against a laptop manufacturer where it turns out, (a)(7) was not even pleaded.²² The best thing that can be said about 1030(a)(7) is that no innocent person has yet been swept up into its prohibitions.

¹⁶ S. Rep. 104-357 at 9.

¹⁷ *Id.* at 11.

¹⁸ *Id.* at 12.

¹⁹ *Id.*

²⁰ *Id.*

²¹ *United States v. Ivanov*, 175 F. Supp. 2d 367, 370 (D. Conn. 2001).

²² *Shaw v. Toshiba Am. Info. Sys.*, 91 F. Supp. 2d 926, 930 n.7 (E.D. Tex. 1999) (noting that Plaintiff did not specify the subsection of section 1030 under which his claim was brought, and summarily describing why (a)(7) did not apply).

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

In part because of the Myth of the Superuser, section 1030 acts as a ratchet, with substantive provisions and criminal penalties that broaden and increase with nearly every Congress. The scenario repeats every two or three years: while the ink is still drying on the last revision to the law, law enforcement officials, led by DOJ, ask Congress to broaden the scope of the prohibition to address the “new threats” on the horizon. Congress ratchets up the law to cover more and more conduct often without credible justification. Meanwhile, once-innocent behavior begins to fall into the new classes of prohibited conduct.

2. Scholars and the Myth: Steganography and IP Spoofing

One way to find examples of scholarly abuse of the Myth is to look for references to oft-misunderstood or overhyped technologies. Steganography is a prime example. A close-cousin of encryption, steganography involves hiding things in plain view. People use steganography software to encode messages or files within other files. For example, text messages can be hidden within image files.

Researchers have developed tools to detect some forms of steganography, but the research is difficult to conduct and unlikely to be very good at detecting new forms of steganography.²³ Almost impossible to detect, the use 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. Because claims about the “widespread use” or “possible use” of steganography are very likely speculative and not founded in statistics or fact, they should rarely be considered effective support for an argument.

Nevertheless, steganography is often cited by scholars trying to prove either: (1) that cunning terrorists are capable of using advanced Internet technology, perhaps in order to justify giving the NSA or FBI more invasive surveillance authority;²⁴ or (2) that new surveillance powers are futile, because criminals will simply turn to more secretive ways to communicate.²⁵ These arguments are abetted by journalists who have written articles

²³ Cf. Niels Provos and Peter Honeyman, *Detecting Steganographic Content on the Internet*, CITI Technical Report 01-11 (2001) at <http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf> (reporting that scan of two million images on eBay had failed to identify any steganographic messages).

²⁴ See Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J. of Nat'l Security L. & Pol. 37 (2005) (former chief of FBI National Security Law Unit arguing that transactional record information is valuable when hunting terrorists because content information can be obscured, for example with steganography); Orin Kerr, *Internet Surveillance Law after the USA PATRIOT Act: The Big Brother That Isn't*, 97 N.W.L. Rev. 607 (2003) (arguing that amending Internet Surveillance laws would help the war on terror because terrorists were known to use advanced Internet technologies).

²⁵ 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 (2002) (arguing against part of the then-proposed UK Anti-Terrorism Crime and

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

about how Al Qaeda or bin Laden *might* have used steganography.²⁶ Again, we'll probably never know.

Another misunderstood Superuser technology favored by law scholars is IP spoofing. IP spoofing helps mask the identity of certain types of attacks against computers. IP addresses uniquely identify computers on the Internet.²⁷ If Person A harms Person B online, an IP address is often the first clue to finding the culprit. If we can't trust IP addresses to be accurate identifiers, we face a crisis that demands resolution.

Sometimes IP addresses can be changed or spoofed, but only by the Superuser. The mere prospect of it sounds terrifying. But many of those who relate this fear leave out an important detail: IP spoofing is not only very hard to accomplish, it is of very limited utility. Spoofing an IP address is a little like cutting your photo out of your passport. You can still use your passport to do some bad things—you can throw it at someone to try to give them a paper cut, or you can burn it to release chemicals into the air—but it's not of much use for getting you through customs into a foreign country. Although I admit that the analogy is strained, the point is that spoofed IP addresses are very good for a few narrow tasks—in particular for being sent as little digital projectiles in a Denial of Service attack—but they are horrible for transmitting communications.²⁸ E-mail messages can't be sent using spoofed IP addresses,²⁹ nor can messages be sent via chat, or songs downloaded through a peer-to-peer network.

Despite the limited nature of IP spoofing, Scholars cite it as a problem encountered online.³⁰ Although they may be referring to exotic attacks that use IP spoofing in

Security Bill because undetectable communication via steganography would remain undetected).

²⁶ Kevin Maney, *Osama's Messages Could be Hiding in Plain Sight*, USA Today at B6 (Dec. 19, 2001) (acknowledging that “no actual evidence has been found of al-Qaeda using” steganography, but stirring the hype nevertheless); Jack Kelley, *Terror Groups Hide Behind Web Encryption*, USA Today at XX (Feb. 5, 2001) (citing “U.S. and foreign officials” for proposition that bin Laden is using steganography).

²⁷ It isn't exactly a unique identifier, but the statement omits some confusing second-order details not important to this analysis.

²⁸ *But see*, *Cert Advisory CA-1995-01 IP Spoofing Attacks and Hijacked Terminal Connections*, <http://www.cert.org/advisories/CA-1995-01.html> (visited July 19, 2006) (describing a technique for taking control of a UNIX computer, “even if no reply packets can reach the attacker.”).

²⁹ In contrast, it is quite easy to send an e-mail message with a spoofed *return address*. IP addresses and e-mail addresses are very different things, and can be used to track online behavior in very different ways. This point is often lost on commentators. [See reporting on *Bulat v. IBM*].

³⁰ See Patricia Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2215 (2004) (listing IP spoofing as one technique used “to impersonate a trusted system.”); Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. Penn. L. Rev. 1003 (2001)

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

conjunction with other techniques to circumvent some forms of security, in context it seems that they are treating IP spoofing as a much more powerful and frequently occurring attack than it really is.

C. Reasons for the Myth

The Myth persists for three reasons: self-interest; the media; and fear of and ignorance about technology.

1. Reason One: Self-Interest

It is often in the self-interest of those who debate or litigate online conflict to portray online actors as sophisticated hackers capable of awesome power. Prosecutors try to paint a picture of their defendants as evil masterminds, to gain jury appeal or even to enhance a sentence.³¹ Law enforcement officials who lobby Congress raise the specter of legions of expert hackers in order to gain new criminal laws, surveillance powers, and additional resources.³² Superusers also provide cover for law enforcement officials who are asked to explain why they don't catch more computer criminals.

Homeland Security officials who specialize in cyberterrorism (a hall-of-fame, Superuser-Myth word) paint a world full of evil, renegade hackers, sponsored by nation-states, and bent on terror and destruction.³³ This elevates their cause in the minds of decision-makers and resource-allocators at a time when other Homeland Security needs press for the same attention. Vendors in the business of selling products and services to protect networks and to combat cyberterrorism echo this worldview.³⁴

In the Digital Rights Management debate, opponents argue that DRM is fundamentally futile because every DRM scheme will eventually be broken.³⁵ Ironically, proponents of DRM (content providers) agree with their opponents that the Internet is full of people bent on breaking the latest DRM;³⁶ this bolsters their calls for increased legal sanctions for DRM circumvention. Opponents of web filtering for libraries or schools argue that filters

(describing the use of IP spoofing “achieve[] entry into sensitive areas or even control of the victim computer by operating privileged protocols”).

³¹ See U.S.S.G. § 3B1.3 (2000) (two-level adjustment for use of a special skill). See also *infra* Part IV.A.1.c (discussing how Courts apply the special skill enhancement in computer crime cases).

³² See Part II.C.1

³³ The President's Critical Infrastructure Protection Board, THE NATIONAL STRATEGY TO SECURE CYBERSPACE 6 (2002) at <http://www.whitehouse.gov/pcipb/> (“Because 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.”) [Comments by Dick Clarke of 2002.]

³⁴ [Press-releases?]

³⁵ See Part III.D.

³⁶ [John Malcolm testimony]

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

can always be circumvented.³⁷ Those against certain types of computerized voting argue that no voting machine security is perfect.³⁸ The examples are nearly endless.

Even though there is merit to some of these arguments, it must be remembered that these partisans and litigants have a vested interest in building up the Myth of the Superuser. By clouding the true impact of the influence of Superusers, these advocates make it more difficult for decision-makers to appreciate the actual state of the world.

Another large group has an interest in inflating the ability of computer criminals: victims. Particularly with computer security breaches, weak network security is often a contributing factor in the success of a breach. Victims are unlikely to admit that their security was weak. Low-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.

Finally, computer criminals themselves tend to inflate the sophistication of their attacks. This is not just an exercise in vanity, as some computer criminals have found that a computer crime conviction can lead to fame³⁹ and riches.⁴⁰ The path to these can be shorter if you are perceived as a criminal mastermind or oppressed genius.

2. Reason Two: The Media

The following headlines appeared in the New York Times in the first seven months of 2006:

- Computer Hackers Attack State Department⁴¹
- Newark: University Computers Hacked⁴²
- Cyberthieves Silently Copy as You Type⁴³
- Your Computer Is Under Attack—LOL⁴⁴
- A Growing Web of Watchers Builds a Surveillance Society⁴⁵

These headlines are fairly representative of a media trend: the hyping of computer crime. It is unthinkable that one would find a story in a mainstream media publication entitled,

³⁷ [Zittrain's empirical work]

³⁸ [Find cite.]

³⁹ [Love Bug].

⁴⁰ [Mitnick.]

⁴¹ Associated Press, N.Y. Times at A6 (July 12, 2006).

⁴² Associated Press, N.Y. Times at B4 (April 10, 2006).

⁴³ Tom Zeller, Jr., N.Y. Times at A1 (February 27, 2006).

⁴⁴ Alex Mindlin, N.Y. Times at C3 (February 20, 2006).

⁴⁵ David Shenk, N.Y. Times at G6 (January 25, 2006).

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

“Most Computer Criminals Use Low-Tech Methods,”⁴⁶ or “Another Unsophisticated Computer Criminal Apprehended,” even if those titles may reflect the truth of the matter.

Reading past the headlines, the reporting about specific computer crimes tends to inflate the sophistication of both the crime and the criminal. Take Kevin Mitnick for example. By some accounts, Mitnick is the most notorious computer hacker in the world.⁴⁷ During his “crime spree” of the late 80’s and early 90’s, Mitnick successfully gained access to numerous computers without authorization. Mitnick’s forte was “social engineering,” which is a glorified term for skillful lying. For example, he once obtained proprietary source code and manuals from [PacBell?] by convincing the person at the front desk of a data center that he was the computer repairman. Although Mitnick possessed some skills that would fit the “Superuser” label, most of his famous attacks relied on social engineering, not technical wizardry.

Despite the low-tech methods used by Mitnick, the media continue to hype him as a sophisticated genius. The New York Times articles written by John Markoff at the time of his storied final arrest breathlessly announces that “[t]he technical sophistication of the pursued and his pursuer [Tsutomo Shimomura, a researcher who help find Mitnick] was remarkable.”⁴⁸ [Get a few more quotes]

Why do the media do this? Computer crime has captured the imagination of many people, as evidenced by the steady-stream of movies⁴⁹ and books⁵⁰ released in the genre. The media probably believe that the public wants stories of daring and intrigue on the Internet. Stories about bumbling criminals using outdated tools captured by untrained law enforcement agents who use traditional methods are less likely to be written or published.

As a result, a spotlight effect distorts the debate. People come to the fallacious conclusion that because they’ve heard about all of these sophisticated hacks in the news, sophisticated hackers must abound.

3. Reason Three: Technological Ignorance and Fear

Finally, compared to what the average lawyer, scholar, judge, journalist, or Congressman knows, everybody online *is* a Superuser. The Superuser Myth is consistent with the

⁴⁶ *But see* Richard Mullins, *Low-tech Hacking*, TAMPA TRIBUNE (Jan. 8, 2006) (describing security-consultant hired to try to social engineer companies’ customers out of their personal information).

⁴⁷ *See* Michael Specter, *An Ex-Con Logs On*, New Yorker (Feb 3, 2003) (“Mitnick, who is usually described as the world’s most notorious hacker . . .”); Patricia Jacobus, *Mitnick Released from Prison*, News.com (Sept. 21, 2000) at (“Kevin Mitnick, one of the world’s most notorious computer hackers . . .”)

⁴⁸ John Markoff, *Hacker and Grifter Duel on the Net*, N.Y. Times A1? (Feb. 19, 1995). Later in the article, Markoff does say that “[i]f anything, Mr. Mitnick’s real ‘darkside’ brilliance comes not from his computer skills, but from his insight into people.” *Id.*

⁴⁹ War Games; Sneakers; The Net.

⁵⁰ Take Down; Hacker Crackdown; Cyberpunk.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

general perception about computers: they are complex machines that only experts can truly control.

There is a kernel of truth in this attitude. Computers and networks are complex devices, and some people are much more skilled at using them (and abusing them) than the average person. But the belief that only experts can abuse computer networks fails to reflect the fact that as software, Operating Systems, and networks have become easier to use, the average user has also become more powerful.

Today, the average, non-expert, non-Superuser computer user can commit computer crimes. Any Internet user can send a bomb threat or extortionate demand via e-mail; collectors of pirated movies or child pornography can use Google to find what they want. Even the term “hacking” has been used to describe the use of a web browser to “access” a public, non-password-protected website.⁵¹

D. The Superuser in the Non-Computer World

Superusers exist in real-world conflicts, too. A small number of people have the knowledge, training, and/or resources to flout technical and legal constraints. Policy makers, however, rarely allow the hypothetical existence of real-world Superusers to distort their deliberations as they do with online conflicts.

Take locks—the physical kind. A small percentage of people know how to pick locks. For the rest of us, locks serve their intended purpose: they keep us out of places we are not meant to go, and they secure things that we might otherwise want to take. Criminal laws have been written that prohibit theft and breaking and entering, and these laws are still considered effective even though some people can pick locks.

Although legislators tend not to fall prey to the Myth of the Superuser in the real world, there is one superficially close parallel: the Myth of the Super-Terrorist. Today’s terrorist is an increasingly mythologized figure whose command over the real world is like the Superuser’s control of the online world. The Super-Terrorist is a master at evasion, able to plan and fund complex crimes without leaving behind any tracks.

The hunt for the Super-Terrorist, it is argued, cannot succeed using outdated surveillance laws and techniques. The old systems for monitoring criminals and spies are ill-suited to deal with the current threat. Because there are so few Super-Terrorists, and because they hide their communications so well among the communications of ordinary American citizens, the laws should be rewritten to allow for warrantless monitoring and widespread monitoring of everybody.⁵²

⁵¹ See Robert Weisman, *Harvard Rejects 119 Accused of Hacking*, BOSTON GLOBE (March 8, 2005) (referring to people who deciphered how to look at public-but-not-yet-advertised parts of a business school admissions website as “hackers” and to their actions as “hacking”).

⁵² See Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST at A31 (Dec. 21, 2005) (commenting that DoD domestic intelligence programs “are criticized as grave

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

Although it is tempting to tie the Superuser directly to the Super-Terrorist, because so many of my conclusions and prescriptions turn on the nature of online technology, nothing more will be said of the connection, except for this: with an increasing frequency, people have begun to talk about the “cyberterrorist,” a person who is *both* a Terrorist and a computer crime Superuser.⁵³ Although there is very little evidence that networked communications (aside from cell-phone calls) have been used to facilitate terrorist acts, these warnings persist. Everything I say here applies with equal or greater force to the Myth of the Cyberterrorist.

III. THE PROBLEM WITH THE MYTH

A. What is Wrong With Believing in the Myth?

There are at least four problems with believing in the Myth of the Superuser and advocating for or passing laws that seek to regulate the Superuser: (1) there aren't many Superusers to regulate and the few Superusers that exist don't exert a lot of influence; (2) their actions defy ordinary metaphors; (3) they often wield power in benign or beneficial ways; and (4) they are very difficult to find and stop.

1. The Hasty Generalization

The principal problem with relying on the Myth of the Superuser is imagining that there are many Superusers when in reality there are few. Another form of this problem is imagining that Superusers have a much stronger impact or reach than in reality they do. Both problems result from a failure to appreciate the empirical reality.

Logicians call this mistake the hasty generalization or the converse accident.⁵⁴ This informal logical fallacy often plagues inductive reasoning from a particular case to a general rule. 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.⁵⁵ It is also a form of another, related logical fallacy known as the appeal to probability. This occurs when the fact that something could happen leads one to conclude that something will happen.⁵⁶

Superusers may walk among us, but they usually do so in small enough numbers as to safely be ignored. Even though a few Superusers can cause harm, they are usually so difficult to find and apprehend; so resistant to ordinary disincentives; or so small a part of the problem as not to be worth the hunt.

threats to civil liberties. They are not. Their significance is in flagging the existence of gaps in our defenses against terrorism.”).

⁵³ See Joshua Green, *The Myth of Cyberterrorism*, WASH. MONTHLY (Nov. 2002).

⁵⁴ See Irving M. Copi, *INTRODUCTION TO LOGIC* xx (4th ed. 1972).

⁵⁵ See *id.*

⁵⁶ Cite.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

Of course, even a few Superusers deserve our attention if they act so powerfully that they account for a significant portion of the harm. This is a form of the more broadly-held idea that some consequences are so terrible that they deserve a significant response even if they are unlikely to occur.⁵⁷ Measuring the impact of the Superuser—as I urge people to do—thus requires more than a head count. The impact turns also on the magnitude of the harm caused by any one Superuser.

Of course, this “principal problem” is only a problem when the underlying facts hold. For some online conflicts, the Superusers may wield a disproportionate impact and thus deserve to be pursued and punished. Deciding whether this is so requires collecting facts that are likely very difficult to discover. In Part IV.A.1, I offer some methods for counting whether a problem is Superuser-rich or Superuser-poor.

But anecdotally, at least some online crimes seem to be committed by ordinary users much more often than by Superusers. Take the growing problem of identity theft. Identity thieves are often portrayed as genius hackers who break into computers to steal thousands of credit cards.⁵⁸ Although there have certainly been examples of criminals who fit this profile, increasingly, the police are investigating and prosecuting people who conduct identity theft in much more mundane, non-Superuser ways. For example, laptop theft is one low-tech way to find information about a person’s identity.⁵⁹ Similarly, some District Attorneys in the Western U.S. have reported that methamphetamine users account for a majority of their identity theft defendants.⁶⁰ Although some of these meth-related cases involve the use of the Internet to facilitate identity theft, they also include non-Superuser techniques such as trash rifling, mail theft, or check washing.⁶¹ Identity theft seems to be a crime perpetrated by ordinary people even though the rhetoric often involves the Superuser.⁶² The Internet may empower desperate people who want to commit identity theft, but these people need not become experts to commit the crime.⁶³

⁵⁷ See Ron Suskind, *THE ONE PERCENT DOCTRINE* at xx (quoting Vice-President Cheney, “If there’s a 1% chance that Pakistani scientists are helping al-Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response.”)

⁵⁸ See Tom Zeller Jr., *Breach Points Up Flaws in Privacy Laws*, N.Y. Times at C1 (Feb. 24, 2005) (quoting Senator Dianne Feinstein saying, “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).

⁵⁹ See David Stout, ‘*Garden Variety Burglary*’ Suspected in Loss of Data, N.Y. Times at A24 (June 9, 2006) (describing theft of laptop containing information about 26.5 million military people).

⁶⁰ John Leland, *Identity Theft Increase Tied to Meth Users*, N.Y. Times at X? (July 11, 2006) (reporting 60 to 70 percent of identity theft cases in Denver tied to meth users or dealers; and 100 percent in Spokane County, Washington).

⁶¹ See *id.*

⁶² There is another way to interpret the anecdotes. DA’s may prosecute meth-addicted identity thieves more often because they are easier to catch than the Superuser identity thieves. See *id.* (“The prevalence of meth use among identity theft suspects may say

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

Putting aside the hard empirical question for now, it is hopefully enough to say that for some types of conflict such as identity theft, the number of Superusers appear to be few. Even if we are unsure whether Superusers are many or few, because of the inherent problems with the Myth that I discuss in the remainder of this subpart, it is wise to place the burden of proof on those who would argue that Superusers have a strong impact on a problem; the presumption should be that Superusers are outliers and that online conflict is more often caused by ordinary actors.

2. Metaphor Failure

The entire field of Internet law can be thought of as a battle of metaphors. When I use your WiFi connection without asking you first, am I essentially trespassing on your property, stealing from your cable company, or walking down the public sidewalk in front of your house? When my ISP reads my e-mail messages, are they acting more like the postman who glances at the backs of postcards or the one who rips open closed envelopes?⁶⁴ Is an encrypted document more like a paper letter inside a closed box or a shredded document?⁶⁵ Superusers upend these analyses, because they defy comparison to the real world.

Superusers can do things with code that have no analogs in the real world. Their acts sound more like science fiction than reality. A hacker can pass through “impenetrable” firewall security (walk through walls) install a rootkit (leave behind no trace) scan entire networks in search of interesting files in a matter of minutes (fly through entire neighborhoods of information) and walk off with millions of identities (thousands of pages of information) never to be heard from again (and vanish). Problems that could be solved if caused by Earth-bound, visible, trackable, ordinary users become intractable when caused by the Supernatural.

When metaphors fail, Internet lawyers and policymakers become deeply unmoored. Having lost their prior points of comparison, they see these conflicts as blank slates, a time to rewrite the rules and start from scratch.⁶⁶ They favor creative and untested solutions and abandon ordinary tools that have been used for decades or longer in real-world conflicts. They ignore lessons learned as irrelevant and forget timeworn rules-of-thumb. These are all forms of an Internet exceptionalism strain of legal thinking that has been debunked by many scholars in recent years⁶⁷ but that stubbornly persists among policymakers and even some academics.

more about the state of law enforcement than about the habits of lawbreakers. In other words, meth users may simply be the easiest to catch.”). *See also* Part III.A.4.

⁶³ Cite to 2004 BH presentation about using Google to find credit card numbers.

⁶⁴ *See* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L. J. 357 (2003).

⁶⁵ *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 884(1995).

⁶⁶ [John Barlow; Johnson and Post.]

⁶⁷ *See* Timothy Wu, *When Code Isn't Law*, 89 VA. L. REV. 679 (2003); Note, James Grimmelman, *Regulating by Software*, 114 YALE L.J. 1719 (2005). I made this point in a

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

3. Guilt by Association

Another mistake made by those under the sway of the Myth of the Superuser is to focus too much on conduct instead of on consequences in defining undesirable online behavior. This mistake is borne of a flawed syllogism: power can be used online to cause harm; Superusers are powerful; therefore, Superusers are harmful. This ignores the fact that many Superusers cause no harm and may even cause great benefit instead.

The result of this type of flawed reasoning is that benign or beneficial Superusers are branded illicit, and in the extreme case, they are sued or prosecuted for doing nothing except wielding their power. This is guilt by association of an especially pernicious and illogical form.

The poster-child for those who have suffered from this type of unfair treatment is Ed Felten, a Computer Science Professor at Princeton University. Felten's research focuses on digital rights management and computer security, and his is an especially applied brand of research that includes trying to circumvent software security products to investigate and prove their flaws. Under threat of a lawsuit, Felten once was forced to delay presenting the results of his past research,⁶⁸ and he now consults regularly with lawyers before undertaking sensitive projects, consuming time and energy that could better be spent on research.

4. Misallocated Resources: Superusers are Hard to Find and Stop

Even when Superusers *are* harming others, because their powers often extend to evading detection and identification, they are very difficult to find and even more difficult to hold accountable for their actions. It is expensive to catch a Superuser. The Department of Justice does a very good job capturing and punishing the dim hackers. The smart ones tend to get away.⁶⁹

Cops need money, time, and tools to find a Superuser.⁷⁰ Given enough of these three things, Superusers can be caught, but for the same amount of money, time, and tools, many more non-Superusers could be found instead.

Even though DOJ tends to capture stupid criminals primarily, whenever DOJ representatives go to Congress to discuss computer crime, they raise the specter of the Superuser criminal.⁷¹ Congress usually responds by increasing the money, time (in the form of FBI and Secret Service agents), and (technical and legal) tools at DOJ's disposal.

student note. Paul Ohm, *Usenet: On Regulating the Internet*, 46 UCLA L. REV. 1941, 194x (1999).

⁶⁸ See John Markoff, *Scientists Drop Plan to Present Music-Copying Study That Record Industry Opposed*, N.Y. Times at C5 (Apr. 27, 2001).

⁶⁹ Find cite or tone down.

⁷⁰ Notice that money, time, and tools are also what can make a criminal a Superuser. See Part I.A. It takes one to catch one.

⁷¹ See, e.g., [notes accompanying Reno hearing testimony.]

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

The result is a shift of resources to the very hardest cases, which may represent only a small percentage of the victims and harm.

B. The Effect of the Myth on Legislation

The four mistakes that result from the Myth—the hasty generalization, metaphor failure, guilt by association, and misallocated resources—lead lawmakers, judges, and scholars to errors of judgment or flawed arguments. Such errors and flaws should be avoided as a general matter, but the Myth spurs specific negative effects that lead to unwarranted government invasions of privacy, inefficient use of law enforcement resources, and bloated, overbroad laws. First, consider what the Myth does to legislation.

1. Overbreadth

Congress's typical response to the Myth of the Superuser is to craft broad laws. Lawmakers amend surveillance laws to give law enforcement new tools for the hunt, even though these laws can also be used to find non-Superusers and to invade the privacy of the innocent. Similarly, Congress broadens criminal and civil prohibitions to cover the hypothetical Superuser. These Superuser-inspired amendments tend to take a specific, especially pernicious form, which I will describe in this section.

Congress overreacts. They imagine the following nightmare scenario: a Superuser will commit a horrific wrong online but will not be able to be brought to justice because of a narrow prohibition in the law. Their cautionary tale is the fate of Onel A. de Guzman, the author of the "I LOVE YOU" virus, which was released in 2000. De Guzman, a Philippine citizen, confessed to writing the virus but escaped any punishment because Philippine law did not criminalize the type of computer harm he had caused.⁷²

In order to ensure that this scenario could not happen here, Congress continuously broadens the scope of its prohibitions. Expansive language is added to anticipate the next, fearsome innovation. New prohibitions are invented to capture hypothetical harms that may never materialize.

When Congress broadens statutes to deal with the Myth, they often cause one particular type of harm that I call investigatory overbreadth. Investigatory overbreadth results from the specific amendments that are often made, and to better understand the argument, a quick detour into the structure of criminal statutes is required.

2. Types of Criminal Elements: Conduct, Results, Intent, Attendant Circumstances

The elements of a criminal statute come in four separate categories: conduct, results (harm), intent, and attendant circumstances.⁷³ For example, under 18 U.S.C. § 2252A(a)(5)(B) it is a crime to possess images of child pornography. The crime is committed by:

⁷² G8 documents.

⁷³ See Model Penal Code § 1.13(9) (classifying conduct elements into conduct, attendant circumstances, and results).

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

[a]ny person who . . . knowingly possesses any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography 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.

Parsing this statute into the four types of elements:

- Conduct element: "possesses"
- Results/Harm element: "any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography"
- Intent element: "knowingly"
- Attendant circumstances: the rest of the prohibition.

When lawmakers succumb to the Myth of the Superuser, they usually focus on *conduct elements*, although sometimes they amend the other three types of elements as well. This makes sense. Conduct is what makes the Superuser unusual, and the power wielded is often itself what some find offensive or threatening. Take two examples from the Computer Fraud and Abuse Act section that prohibits damaging computers. Under section 1030(a)(5)(A)(i), the prohibited conduct is “caus[ing] the transmission of a program, information, code, or command.” This is a sweeping conduct element that is never more precisely defined in the statute. It would appear to encompass any type of network communication.

Similarly, under section 1030(a)(5)(A)(ii), the conduct proscribed is “access[ing] [a protected computer] without authorization.” Access is not defined, and neither is “without authorization.”⁷⁴ These vague terms of prohibited conduct have been litigated often, usually in the civil context, with most courts giving them a broad application. [Describe McDanel case] [Describe Explorica case]⁷⁵

3. The Investigatory Funnel

As a result of Congress’s tendency to expand the conduct elements of these prohibitions, conduct is no longer a meaningful, limiting principle of many of its computer crimes.

⁷⁴ See Part III.B.3.

⁷⁵ As another example, consider the Wiretap Act. The 1986 Electronic Communications Privacy Act extended the prohibitions in the Wiretap Act to electronic communications; presumably, computer wiretaps are now illegal. Again, the conduct proscribed is broadly defined; 18 U.S.C. § 2511(1)(a) makes it a crime to “intercept[] an . . . electronic communication.” “Intercept” means the “acquisition of the contents of any . . . electronic . . . communication.”

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

The Superuser's conduct is hard to define, so Congress gives up trying. If you "transmit" or "access," you have satisfied the conduct elements of the crime. As a result, these elements no longer serve to discriminate between good behavior and bad. They are merely low hurdles that when cleared place your acts within the general reach of the prohibitions. This is why the FBI could claim that McDanel "transmitted information" when he sent e-mail messages to his former employer's customers. Likewise, the web scraper in Explorica Travel "accessed without authorization" the price information of its competitor, even though it merely downloaded information from a public website.

Why do broad conduct elements result in overbroad laws? What about the other three types of criminal law elements? Specifically, why don't narrowly written harm and mens rea elements protect innocent, nonculpable actors? Even if someone "accesses without authorization" a computer, so long as damage doesn't occur or intent is absent, aren't the deservedly nonculpable never convicted?

These arguments fail because they focus only on the question of indictment or conviction.⁷⁶ Laws with narrow harm and mens rea elements but broad conduct elements are likely to trigger broad police investigations into the behavior of many innocent people. If wrongful investigation concerns us nearly as much as wrongful indictment or conviction—and I think it should—then this is a problem.

By "overbreadth," people usually mean what I call prohibition overbreadth: a criminal law is overbroad if it labels acts culpable that are beyond the original intent, policy justifications, and harms that the drafters envisioned when they wrote the law. If the drafters meant to punish those who do X and the law can be used to punish those who do Y (where Y is not X) then the law is overbroad. Narrowly written harm or mens rea elements can help avoid prohibition overbreadth.

Criminal laws can also be harmfully overbroad when *the very structure of the laws* leads to prolonged and unjustified investigations of the innocent. This is another class of

⁷⁶ These arguments fail for a second reason: Congress sometimes broadens harm elements in response to the Myth of the Superuser. Superusers break things in unforeseeable ways. Take another example from the CFAA. Under section 1030, "damage" is anything that impairs the "integrity or availability of data, a program, a system, or information." Taken at face value, it is criminal damage to choose one file out of the tens of thousands on a computer server and modify one comma out of the thousands of characters in that document. Again, Congress kept the definition vague and broad to try to encompass any clever, devastating attacks that would be wrought by the Superuser.

Congress did limit damage by further requiring statutory loss, which is defined as one of five types of loss. See 1030(a)(5)(B). Some of those types are very broad, for example, "damage affecting a computer system used by or for a governmental entity in furtherance of the administration of justice, national defense, or national security." See 1030(a)(5)(B)(v). So modifying one character in one file on a computer used by an administrative assistant at DHS may suffice.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

overbreadth, which I call investigation overbreadth.⁷⁷ In other words, some criminal law elements are written so broadly and vaguely that they trigger police scrutiny of purely innocent behavior.

To better understand investigative overbreadth, envision the process of narrowing down the suspects of a crime as a graph of the “investigative profile,” with time moving along the x-axis and the number of suspects along the y-axis. The graph looks like a funnel. The wide end of the funnel is the pool of everybody who could possibly have committed the crime at the very start of the investigation. In some instances, the wide end of the funnel may be “every computer user in the world”. The narrow end of the funnel is the goal—the identification of the specific person or persons who committed the crime.

To see how statutory structure dictates the shape of the funnel, consider the chronological order in which the elements of a crime are usually established during a criminal investigation. The facts establishing harm elements are usually the first known; except in the case of inchoate crimes, the dead body, missing jewels, or burned warehouse are the reason the police are called. For online crime, the unresponsive web server, death threat e-mail, or downloadable copies of the DVD are the first indication of a crime.

At the other end of the spectrum, the mens rea elements are usually the last piece of the puzzle established, only after the suspect is identified and the witnesses interviewed. Prosecutors can often be found shoring up their mens rea evidence—most of it circumstantial—even on the eve of trial. If our goal is to reduce the number of wrongful investigations, harm and mens rea are poor limiting principles.

A criminal law that suffers from investigative overbreadth triggers investigation profiles with long, wide funnels that narrow only after significant amounts of time have passed. At the wide end of the funnel, the police have no choice but to subject many innocent people to their scrutiny and for a long period of time. This type of harm is multiplied with online crime, because the police can efficiently, quickly, and deeply probe into the private lives of many suspects. They don’t need to knock on neighbors’ doors and dig through the trash; the same type and amount of information yielded with such real-world techniques can be replicated by a few subpoenas to a half-dozen ISPs.⁷⁸

For example, consider the unresponsive web server mentioned above. The computer crime officer called to the scene knows immediately that the harm element of section 1030(a)(5) has been met—the server is “damaged” and it is easy to establish that the loss suffered by the server’s owner amounts to more than \$5000.⁷⁹ With no obvious suspects, the investigation begins. Situated at the wide end of the funnel, the police ask, who in the

⁷⁷ I don't necessarily mean overbreadth in the Constitutional sense of the word, but instead I refer to a judgment about criminal laws that are socially unwise.

⁷⁸ See Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 SO. CAL. L. REV. 1083, 1084 (2002).

⁷⁹ 18 U.S.C. § 1030(a)(5)(A), (a)(5)(B).

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

world could have caused this harm *and* any of the conduct elements required by the definition of the crime?

Broad conduct elements mean large suspect pools. Because the statute broadly applies to those “without authorization” and “in excess of authorization,” both insiders and outsiders need to be considered; the funnel remains wide. It could have been a teenager in Europe launching a denial of service attack, it could have been a cyberterrorist hacking into the server directly, or it could have been a faithless employee abusing his privileges.

Because the Explorica court construed “without authorization” to apply to those who merely breach contractual duties, the seemingly benign acts of all employees and contractors need to be scrutinized. Because the McDanel court held that merely sending e-mail messages to third parties can constitute the “transmission of information,” the private e-mail messages or instant messages of customers and other outsiders should be scrutinized.

Conduct elements that have been broadened to deal with the Superuser thus provide no limit to the number or type of people who are suspects; they do not narrow the funnel at all. At the same time, these broadly defined conduct elements make it easy for the police to establish probable cause to search the e-mail inboxes, web surfing habits, and maybe even the real-time communications of some or all of their suspects, including all three of the people described above. Because most of the Internet surveillance laws do not require notice to the surveilled party,⁸⁰ law enforcement officials can learn about the private acts of dozens or more people without jeopardizing the investigation. The confluence of broad prohibitions with lax surveillance laws gives the police both the incentive and the means to use bigger and more invasive dragnets.

These wide-end funnel investigations also represent wasted police resources. If distinguishing between the culpable and nonculpable turns on investigating every suspect’s mens rea, then the police must stay with more leads for more time.

As the unresponsive server example demonstrates, conduct elements dictate funnel shape much more than harm elements or mens rea elements. If Congress made clear that certain crimes can only be conducted by outsiders,⁸¹ the funnel would become significantly narrower. If Congress made clear that “transmitting information” does not apply to e-mail communications, *contra* McDanel, the funnel would also narrow. But Congress is loath to narrow conduct elements in this way, not necessarily because it is convinced that insiders or people like McDanel deserve punishment, but because they worry that a Superuser’s metaphor-busting acts will slip outside a narrow prohibition.

⁸⁰ See, 18 U.S.C. § 2703(b)(2); 2518(?); 3123(?). *But see* 18 U.S.C. § 2703(b)(1).

⁸¹ See, e.g., 18 U.S.C. § 1030(a)(3) (defining criminal attacks on government systems to exclude certain insiders); 18 U.S.C. § 1030(a)(5)(A)(i) (defining non-access attacks on protected computers to apply only to outsiders).

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

C. The Effect of the Myth on Judges

1. Judges and the Myth

Falling sway to the power of the myth is not just for legislators; Judges also accept arguments premised on the existence of a class of Superusers who cannot be constrained by ordinary laws.

[Any time a Judge is asked to construe a law defining the “reasonable computer user” or the “standard of care” involving a network, the Judge is susceptible to the Myth. The reasonable, average computer user’s abilities may be inflated if the Judge believes that Superusers permeate the universe of users. A standard of care may be unduly stringent if the acts of the Superuser are considered.]

2. Example: Search Warrants for Computers

Search warrants for computers are a prime example. The Magistrate Judges who sign these warrants and the District Court Judges who review the searches that result usually allow sweeping and highly invasive searches justified by stories about one type of Superuser: the Data Hider.

It has become standard practice for agents in affidavits in support of computer search warrants to talk about the sophisticated technology that can be used to hide data.⁸² Criminals “have been known” to use steganography, kill switches, and encryption to hide evidence of their crimes. Agents need to recite these words because courts have repeatedly held that each file in a computer is a separate “container” over which a person ordinarily has a Fourth Amendment reasonable expectation of privacy and for which the police must establish independent probable cause to open.⁸³

As a result, a typical computer warrant authorizes the search of every single file on the computer. Furthermore, because the data hider can store evidence in obscure places, such a warrant also authorizes the search of parts of the hard drive that don’t even store files and that are usually unknown to most computer users such as the swap file, deleted space, file slack and RAM slack. Arguments about how expert data hiding are also used to justify off-site computer searches, where data is forensically examined for months or maybe even years.

If in reality criminals “have *not* been known” to hide data in files with obscured names and within encrypted bundles, then Magistrate Judges might ask the police to “cordon

⁸² Computer Crime & Intellectual Property Section, Criminal Division, U.S. Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, App. F (2002) [hereinafter DOJ Manual], available at <http://www.cybercrime.gov/s&smanual2002.htm> (offering a model search warrant that includes language to justify an off-site search, “data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even “hidden,” erased, compressed, password-protected, or encrypted files”).

⁸³ See *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999); Orin Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 554-57 (2005).

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

off” parts of a computer's hard drive. The law enforcement community greatly fears such a result,⁸⁴ because current computer forensics techniques usually treat the entire computer's hard drive as a unitary pool of data through which to search.⁸⁵

The hypothetical expert data hider, cognizant of every trick that can be used to hide contraband and other evidence, is the classic Superuser. Common sense suggests that some criminals are paranoid enough to hide evidence. Common sense also suggests that other criminals probably aren't so paranoid. Home computer users who are committing relatively nontechnological crimes—tax fraud or extortion, 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 case study in the Myth.

By believing that every computer user in every warrant application is a potential Superuser data hider, Magistrate Judges may not be giving sufficient respect to the Fourth Amendment rights of those searched. In some cases, constraints on the scope of the search of a hard drive may be sensible, and perhaps Constitutionally mandated. For example, in a search of a hard drive for evidence of music illegally traded over peer-to-peer networks, it may make sense to limit the police to search only in the computer directories used by the software to access those peer-to-peer networks. Just as a warrant to search for a gun cannot be used to support the search through the stacks of paper on a desk,⁸⁶ nor should agents be allowed to look for music where it cannot be found.

The consequence of allowing computer-wide searches in every case can be grave. As the capacity of hard drives grows, the incentive for computer users to delete old files diminishes. Today's hard drives store quantities of information that are unprecedented compared to paper-based filing systems of the past. Today's computer can contain tens of thousands of letters, e-mail messages, business records, and financial documents, stretching back years. Given the way that the plain view rule has been interpreted in the computer context,⁸⁷ evidence of any crime found during a computer search can be used to prosecute the computer's owner for a crime unrelated to the crime recited in the warrant. Succumbing to the Myth in this case gives law enforcement the power to search that seems inconsistent with traditional Fourth Amendment limits.

⁸⁴ See Kerr, *supra* note 84 at 576 (“The computer forensics process calls for ex post standards, not ex ante rules.”).

⁸⁵ See *id.* 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.

⁸⁶ [Find case.]

⁸⁷ See Kerr, *supra* note 84 at 576.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

D. The Effect of the Myth on Scholars

Like lawmakers and Judges, scholars invoke the Myth of the Superuser in unwarranted ways.⁸⁸ Scholars misuse the Superuser in two broad, overlapping situations. First, they

⁸⁸ A few scholars have discussed the Superuser in sympathy with my current argument. Larry Lessig has repeatedly 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. As far back as 1996, Lessig argued that:

But 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. Locks, like security systems on computers, will be quite effective, even if there are norm-oblivious sorts who can break them.

Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 896 n.80 (1996). See also Lawrence Lessig, *Constitution and Code*, 27 CUMBERLAND L. REV. 1 (1996-97) (“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 COMM. L. CONSPECTUS 181 (1997); Lawrence Lessig, *The Zones of Cyberspace*, 48 Stan. L. Rev. 1403, 1408 n. 17 (“[What] hackers do doesn't define what the effect of law as code is on the balance of the non-hacker public.”).

Even if hackers cannot be regulated, there is still a need for regulation, according to Lessig, because the aim of the law is to regulate enough behavior to accomplish a goal, not to stamp out the harm entirely. See Lessig, *supra* note 51, 48 Stan. L. Rev. at 1408. Tim Wu echoed a similar point in addressing the Myth in an early essay. He observed that:

From the beginning, it was clear that the descriptive argument—the claim that Cyberspace cannot be regulated—would fall moot. This old cyberlibertarian bromide self-destructs under the glare of technical scrutiny and the simple recognition that regulation need not be perfect to be effective—that regulation works through transaction cost rather than hermetic seal. Consider 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. Cyberlibertarians, some of whom have the Internet skills equivalent to the real-space locksmith, generalize from their own experience to conclude that no regulation of Cyberspace is possible. But neither the theory nor the results are convincing—if regulation is impossible, then what are criminal hackers doing in prison?

Timothy Wu, *Application-Centered Internet Analysis*, 85 VA. L. REV. 1163, 1195-96 (1999). Wu continues, in the conclusion of the same essay, to say:

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

use the Superuser *defensively* to argue against positions by noting that the Superuser has powers that weaken or contradict arguments. Defensively, the Superuser is the *deus ex machina* of legal scholarship, drifting down from the rafters to wipe away nettlesome arguments with a wave of its arm.

Second, scholars use the Superuser *offensively*, to support arguments or positions and to advocate for changes to laws, helping the Scholar zip past weaknesses in an argument. In either case, Scholars side-step important dimensions of the debate unless they expressly acknowledge that the force of these arguments depend on facts about the prevalence of the Superuser.⁸⁹

The latest rounds of Internet sloganeering have been the talk of a funny kind of vested interest-- not the usual suspects, but a kind of Madisonian notable of the computer age best known as the "expert user." . . . [E]xpert users suffer least and benefit most from an unregulated Internet. Remember, after all, who actually uses encryption software and who still needs help opening attachments; who knows what mp3s are and how to get them and who just pays more for CDs at the store; and, of course, who knows how to disable Microsoft Explorer's domination of the desktop and who ends up stuck with it. The truth is that normal users might one day (or perhaps now) want the help of their government in some or all of these areas. . . . [T]o stick everyone with the constitution of the expert user may, in the long run, prove the inept move, as it may do more to close out the Internet than flexibility ever would.

Id. at 1203.

Wu and his co-author, Jack Goldsmith, make a similar point repeatedly in their recent book on the state-control and regulation of the Internet. *See, e.g.,* Jack Goldsmith and Tim Wu, *WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD* 123 (Oxford 2006) (predicting a world in which a minority users "with all the time and expertise" continue to download free music while the rest use legitimate pay sites).

These and other scholars, *See* Jessica Litman, *DIGITAL COPYRIGHT XX*, have raised the problem of confusing the needs of experts with the needs of ordinary users. However, none has dug deeper into this observation, to examine the negative effects that result from relying on the Myth or to provide detailed prescriptions for dealing with these effects.

⁸⁹ I have found that student note authors seem to fall prey to the Myth more often than their counterparts in the Professorial ranks. *See, e.g.,* Note, Stephen W. Tountas, *Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?*, 11 Wash. U. J. L. & Pol. 351, 376 (2003) ("Given the devastation of September 11, along with sophisticated tactics such as steganography, it is in Congress' best interest to disregard Carnivore's constitutional issues"). 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.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

For examples of both offensive and defensive uses of earlier scholarship, consider the debate over the Digital Millennium Copyright Act (“DMCA”) and Digital Rights Management (“DRM”). The DRM debate is suffused by the Myth. Critics of DRM regularly point to a paper written by four Microsoft engineers entitled “The Darknet and the Future of Content Distribution”⁹⁰ as proof of the ineffectiveness of laws like the DMCA.

The first premise of the Darknet paper is the sentence most often misused: “[a]ny widely distributed object will be available to a fraction of users in a form that permits copying.” In other words, in the battle between lock builders and lock pickers, the Darknet authors start from the assumption that the lock-picker Superusers have the upper hand.

Those who cite this premise often miss the fact that it is but “an assumption.” The authors do not attempt to prove the assumption with rigor, but instead take it as a starting point. Others, however, have cited the first premise of the Darknet paper as proven fact,⁹¹ which it is not, at least not in this paper.

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* the Superusers have acted. Their central argument is 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] today.”⁹² 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 there are some Superusers feeding these darknets (again, this is just an assumption), these darknets will thrive and will also be very difficult to detect and shut down. People who cite the Darknet paper often mistake the starting point for the conclusion.

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. The authors do not contend (nor could they) that the Superusers of the world have the skill, time, and interest to break every single piece of DRM-protected content. Theirs is a more

⁹⁰ See Peter Biddle, Paul England, Marcus Peinado & Bryan Willman, *The Darknet and the Future of Content Distribution* (2002), available at <http://crypto.stanford.edu/DRM2002/darknet5.doc>. The person 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)

⁹¹ See Von Lohmann, *supra* note 90 at 640; Julie Cohen, *The Place of the User in Copyright Law*, 74 Fordham L. Rev. 347, 361 (2005); 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).

⁹² Biddle et al. *supra* note 90 at xx.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

modest point about incentives. The premise is studded with caveats: only works that are “widely distributed” satisfy the claim; only a “fraction of users” (how large a fraction?) can copy these works; even vulnerable works “permit[] copying” but won’t necessarily be copied.

In other words, DRM-protected copies of obscure, nonpopular music may never fall into darknets, because no Superusers will be incentivized to break the unlock them. Likewise, even for popular content, there is a bandwidth problem: Superusers can break DRM only at a fixed rate, and some of these DRM schemes are difficult to break. Even popular music may have to wait in a queue for an interested Superuser to come along.⁹³ For some content owners, DRM systems that are not broken for months or years are good enough,⁹⁴ especially because users can be convinced or forced to upgrade to newer, stronger versions of DRM schemes once the older version is broken.⁹⁵

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 . . .,” although they speculate that this is because most DRM-protected content is uninteresting. This point—that DRM is often good for a few months head start—is almost never cited. In the conclusion, the authors go so far as to say that if darknets tend to be isolated from one another (a possibility the authors seem implicitly to doubt) then “even BOBE-weak DRM [referring to a particularly weak class of DRM] systems are highly effective.”⁹⁶

⁹³ See Nate Anderson, *Hacking Digital Rights Management*, <http://arstechnica.com/articles/culture/drmhacks.ars> (July 18, 2006) (noting that Microsoft’s DRM system for audio “has not been widely breached” since late 2001)

⁹⁴ See *id.* at <http://arstechnica.com/articles/culture/drmhacks.ars/4> (noting that even imperfect DRM schemes “may be good enough for most [record] labels”).

⁹⁵ See Zittrain *supra* note 6 at 2019; 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)

⁹⁶ The authors are also fairly nuanced about different categories of DRM, some of which they think are hopelessly flawed and others that merit more optimism. For example, the authors are clearly unimpressed by watermarking technology—schemes to encode data in content that can’t be perceived by the ordinary viewer or listener, but that can be used to “mark” a copy as legitimate or not. A watermark can tell an advanced music player, for example, that a particular copy of a song cannot be played until the user enters a password. In criticizing watermarking, the authors point to two, technical flaws -- it is very easy to “strip” watermarks, even if you don’t know exactly how they were encoded; and most watermarks use easy-to-evade encryption schemes.

In contrast, fingerprinting schemes—using marks to stamp a copy with information identifying the purchaser to allow for after-the-fact punishment for illegal copying—are more promising. “Fingerprinting suffers from fewer technical problems than

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

Finally, those who cite the Darknet paper forget that its authors are optimistic even 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. The paper seems decidedly pessimistic about the ability for a centralized service such as these to resist legal challenge for long. Even the DMCA is called a “far-reaching (although not fully tested) example of a law that is potentially quite powerful.”

To be sure, the Darknet paper casts serious doubts on the ability of DRM to stop all copyright infringement. The paper's authors try to temper expectations that laws like the DMCA will be a “silver bullet” against the spread of unauthorized copies of copyrighted works. In the debate over DRM, this 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 of the Superuser. The sound-bite version of the paper's conclusion is the claim that “powerful users will circumvent any protection scheme released.” This sound-bite is intuitive, appealing, and wrong.⁹⁷

IV. PRESCRIPTIONS, ADDITIONAL DIFFICULTIES, AND FUTURE WORK

A. Prescriptions

1. The Facts Behind the Myth

Because the Superuser Myth often inaccurately describes the state of the world, the antidote is better fact-finding. People should resist the urge to raise the specter of the Superuser when talking about online conflicts unless they are prepared to answer three separate questions with respect to the particular conflict: How many users—in raw numbers and as a percentage of the population—are currently Superusers? How easy it for ordinary users to become Superusers?⁹⁸ How powerful are the Superusers that exist?

Obviously, for some types of online conflict these questions will be unanswerable even in approximation; for most types of conflict, the questions will be very difficult to answer accurately. Three sources can be consulted to develop a more accurate picture of the world: statistics; experts; and if all else fails, anecdotes and intuitions.

watermarking.” Although the paper still raises some technical challenges, the authors are much more optimistic about its viability as a strategy.

⁹⁷ In fact, the paper itself is a good model of a measured, careful way of dealing with the Superuser. The paper calls in its last section for further empirical work about the nature of the darknets, consistent with my recommendation in Part IV for a more searching empirical inquiry to back up Superuser claims.

⁹⁸ The answer to this question will change over time. The more complete inquiry is: How many ordinary users easily can become Superusers today? Is something likely to change in the future that will empower more users to become Superusers?

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

a. Statistics

Statistics may help calculate the ratio of Superusers to non-experts in an online conflict. Unfortunately, meaningful statistics measuring even the basic occurrence of online crime simply do not exist,⁹⁹ so it is optimistic to expect even better statistics that break down the number of Superusers. Nevertheless, some rarely-tapped sources for counting Superusers hold some promise.

A study of prosecutions and investigations can help quantify the breakdown in expertise of those caught and punished.¹⁰⁰ Naturally, a measure of a defendant's expertise is not likely to be collected for many crimes, so the analysis may require a closer study of indictments, published opinions, or news reports.

[The problem with studying prosecution and investigation statistics is that the results may be ambiguous. If the FBI investigates and prosecutes only amateurish child pornography traders, it may be because child pornography traders tend to be non-expert, or it may be because the sophisticated child pornography traders cannot be found or brought to justice given the FBI's resources and tools. One way to disambiguate this result is to compare these statistics against civil lawsuit filings, at least with prohibitions that provide both criminal and civil relief. So, for example, if both civil hacking lawsuits and criminal hacking prosecutions under section 1030 tend to be brought against non-Superusers, it strengthens the conclusion that expert Superusers are not very prevalent.]

Statistics are also collected by organizations that monitor various online harms. Companies that write virus scanning software keep statistics about virus activity.¹⁰¹ Companies that sell firewalls summarize the types scans and intrusions seen by their customers.¹⁰² The RIAA and MPAA both monitor peer-to-peer networks with advanced data-collection "spiders" to track the distribution of their copyrighted works on those networks.¹⁰³ Other sources include disinterested, non-commercial entities such as the SANS Internet Storm Center [Choose a better candidate] which collects information about threats on the Internet.¹⁰⁴ The HoneyNet Project is a collection of volunteers who set up purposefully-vulnerable computers on the Internet to monitor and profile a "typical" intrusion.¹⁰⁵ Any of these sources of information can help breakdown online threats by attacker level of sophistication.

⁹⁹ See Susan Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 Vand. J. L. & Tech. 13, *3 & n.3 (2004) (noting that there are no "measures and benchmarks for the incidence and damage caused by" computer crime).

¹⁰⁰ [See NY Times article about meth users/ID theft]

¹⁰¹ Symantec website or white paper.

¹⁰² Zone alarm paper.

¹⁰³ Verizon opinion? Grokster opinion?

¹⁰⁴ SANS website.

¹⁰⁵ HoneyNet website.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

b. Experts

[Computer Scientists have conducted research into online conflicts that has largely been ignored by those in law. Computer Scientists, for example if called before Congress, can help dispel or confirm the fear that virus writing—for example—is the province mostly of a few experts.]

There is precedent for this type of analysis; Judges sometimes turn to experts to assess the level of sophistication of a computer crime during sentencing. Section 3B1.3 of the Sentencing Guidelines provides that, “If the defendant . . . used a special skill[] in a manner that significantly facilitated the commission or concealment of the offense, increase by 2 levels.”¹⁰⁶ The commentary elaborates, “‘Special skill’ refers to a skill not possessed by members of the general public and usually requiring substantial education, training or licensing. Examples would include pilots, lawyers, doctors, accountants, chemists, and demolition experts.”

When prosecutors seek Section 3B1.3 enhancements in computer crime cases, Judges are asked to determine whether the crime required “a skill not possessed by members of the general public and usually requiring substantial education, training, or licensing.” To do so, they often look to experts. For example, in *U.S. v. Lee*,¹⁰⁷ the Ninth Circuit reversed the application of the enhancement. Lee had defrauded people by creating a website designed to mimic the website of the Hawaii Marathon in order to fraudulently obtain registration fees from would-be marathon runners. The skill in question was the detailed copying of the original website.

The Ninth Circuit referred to the testimony of the designer of the Marathon website Lee had copied. That person, obviously experienced although not certified as an expert, described ways to use off-the-shelf software to copy a website. The Ninth Circuit credited this testimony and even cited a computer book that the witness had testified could have been used to assist an average user to achieve this result.¹⁰⁸

¹⁰⁶ U.S.S.G. 3B1.3.

¹⁰⁷ 296 F.3d 792 (9th Cir. 2002).

¹⁰⁸ Unsurprisingly, not every 3B1.3 analysis is as rigorous. For example, in *U.S. v. Prochner*, 417 F.3d 54 (1st Cir. 2005) the First Circuit affirmed the application of the enhancement because the defendant “hacked” into website order logs and re-wrote “cgi scripts.” The court felt that “[e]ven without expert evidence” the Defendant’s own admissions to the police evinced special skill. The court seemed most swayed by two jargon-filled paragraphs written by the defendant himself admitting what he had done. The court made no attempt to translate the jargon. The court was convinced of the defendant’s skill, at least in part, because one of the self-described acts was called a “hack.” Based on the admissions alone, the court held that the defendant’s skill to be “well beyond that of a member of the general public.” *Id.* at 62.

This is not to say that Lee was correctly decided and Prochner incorrectly decided. Prochner’s actions appear to be more sophisticated than Lee’s, and at the very least, the holdings seem to stem from a Circuit split in the interpretation of 3B1.3.¹⁰⁸ The point is

c. Anecdotes and Intuitions

Although too much can be made of anecdotes and intuitions, consulting them about the prevalence of Superusers is likely to be more useful than the current, uninformed status quo. Intuition suggests that Superusers tend not to have a significant impact on most online conflicts. This intuition stems from the answers to questions such as: How difficult is it to cause the type of harm at issue? (If it is not very difficult, intuition suggests that the ability to commit the harm is not limited to Superusers.) Does the harm require advanced computer programming, or is it something that a simple script can accomplish? How sophisticated are the counter-measures to the harm? (This in turn suggests questions like, how large is the counter-measure creating community? How advanced and organized are its members?) Have Superusers automated the tools required to cause the harm? Are these tools easy to use? Are these tools easy to find?

For example, take virus writing. An informed observer would make these observations about the ease with which new, destructive viruses can be released: First, up-to-date virus checkers do a pretty good job of mitigating the risk of infection from past viruses.¹⁰⁹ Second, computer users who diligently install Operating System patches and software updates are relatively immune to new viruses. Third, against computer users who are diligent about updating their virus software, Operating System, and other software, infection will probably only come from new viruses written to exploit new vulnerabilities. Fourth, only expert Superusers with significant computer programming ability, a lot of spare time, and access to other would-be attackers will succeed in infecting these machines.

Intuition might suggest, based on this analysis, that only expert Superusers can create catastrophic viruses. On the other hand, this back-of-the-envelope analysis misses perhaps the most relevant observation: many (most?) people do not update their virus checkers and do not diligently install system patches. Against these “victims,” non-expert attackers using old tools, some of which are packaged in easy-to-use software, can successfully infect. The intuition swings back to supporting the idea that virus writing is a field in which ordinary users can do great damage.

As this discussion demonstrates, the anecdote/intuition analysis cannot answer definitively whether to be concerned about the Superuser, but even this level of analysis is better than the blind conclusion that virus writers are all Superusers.

2. Advice for Lawmakers, Judges, and Scholars

Armed with better facts about the impact of the Superuser, what should a conscientious lawmaker, judge, law enforcement officer, or scholar do? First, for a given conflict, if the facts confirm my prediction that Superusers are few and have little aggregate impact, the

that the Lee court assessed the skill of the defendant with much more rigor and much less technophobic awe than did the Prochner court.

¹⁰⁹ [Felten’s blog post or something from the CS literature]

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

conscientious person should act as if the Superuser does not exist. If a conflict involves ordinary users in the main and Superusers only at the margins, too much focus on the few will distort the debate for the reasons I have discussed above.

a. For Lawmakers

Legislators should craft narrow prohibitions that seek to regulate the predictable and understandable actions of the ordinary user; metaphors will be easier to spot and more convincing and can be used to borrow approaches taken in other areas of law. On the search and surveillance side, lawmakers should resist calls to provide new powers and to carve new exceptions out of pre-existing privacy laws that assist in the hunt for the Superuser.

Returning to an earlier example, Congress should be loath to continue applying the breadth-and-vagueness ratchet to section 1030. For example, it is conceivable that DOJ might ask for a loosening of the “loss” requirement in 1030(a)(5). Recall that damage to a computer is only criminal with sufficient loss, which for many cases means the victim must have suffered more than \$5,000 over the course of the attack.¹¹⁰ DOJ might argue that the \$5,000 limit is an anachronism, because recently, Superuser attackers have been known to attack thousands of separate victims, creating “bot armies” of computers to use at a later time.¹¹¹ Even though the damage done to any one computer is much less than \$5,000, and even if the total loss cannot be aggregated to equal \$5,000, the harm to the network (and to society) is great.

If DOJ does come calling with this story, Congress should not react to the Myth of the Superuser “General of the Bot Armies” by striking the \$5,000 threshold, because the threshold serves an important purpose: it minimizes trivial prosecutions. Many annoying-but-not-devastating acts occur on the networks every day. Automated search engine programs accidentally delete data from poorly-configured websites;¹¹² spam filters delete non-spam; practical jokes are played in offices on co-workers. None of these “ordinary user” acts are typically prosecuted, even though they may fall within the broad

¹¹⁰ Congress has tightened the ratchet relating to the \$5,000 several times. Initially, the requirement was “...” and had been interpreted to mean that an individual victim had to suffer \$5,000 worth of loss due to a single incident. [Case]. In 199x, this was amended to make clear that the \$5,000 could be suffered over a course of many months, due to an ongoing attack.

¹¹¹ U.S. Dep’t of Justice, *Computer Virus Broker Arrested for Selling Armies of Infected Computers to Hackers and Spammers*, <http://www.usdoj.gov/criminal/cybercrime/anchetaArrest.htm> (November 3, 2005).

¹¹² Google sends out automated programs called “spiders” to collect information about the content on the world wide web. In early 2006, it was reported that the Google spider “clicked” on a “edit content” button which, poorly configured, erased all of the content on the website. See Nick Farrell, *Beware the Google Spider*, THE INQUIRER (March 30, 2006) at <http://www.theinquirer.net/default.aspx?article=30640>.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

and vague conduct elements of section 1030(a)(5).¹¹³ The reason prosecutors and agents quickly decline these cases is due to the \$5,000 loss threshold. This is a good thing.

If Congress were to remove the \$5,000 requirement, then over-zealous prosecutors and agents would be free to bring charges against harmless users like those listed above. Even if these prosecutors and agents never decided to charge a crime, they could still subject these people to invasive search and surveillance. If Congress were to remove the \$5,000 loss requirement, even the mere office prankster's actions would establish probable cause for the FBI to search his e-mail accounts, computer, office space, and maybe much more.

b. For Judges

Similarly, Magistrate Judges should give greater scrutiny to unsupported claims that the Superuser data hider is everywhere and that his powers justify sweeping searches and unconstrained surveillance. These claims are not limited to the affiant statements about obscured filenames that were discussed in Part III.C.2. The threat that a computer may be "wired to self-destruct" is often used to justify an exception to the knock-and-announce requirement, even though the actual reported incidence of booby-trapped computers is low. The concern that criminals sometimes encrypt their files is used to justify the installation of key logging software.¹¹⁴

Of course, what an agent says in an affidavit is owed deference under ordinary Search Warrant principles, but deference is not turning a blind eye to obvious overstatements. Just because the agent asserts based on years of training that people wire computers to self-destruct, a Magistrate Judge should dig deeper into the affiant's knowledge of these past cases.

Judges who encounter the Superuser Myth in affidavits should consider two counter-arguments. First, different types of crimes lend themselves to different levels of data hiding. Second, the Superuser Myth should be offset by the reality of the Super-investigator.

I doubt that all criminals are equally good data hidiers. Experience has probably shown that sophisticated criminals who break into networked computers tend to hide their evidence.¹¹⁵ For search warrants relating to these crimes—with a demonstrably provable past history of being performed by Superusers—the Superuser Myth is not a myth, and investigators should be granted broad warrants to look throughout the suspect's entire hard drive. But I speculate that the same cannot be said of those who violate copyright laws or who commit frauds. Warrants to search for evidence of these types of crimes

¹¹³ Section 1030(a)(5)(A)(iii) criminalizes access that leads to damage and has no mens rea requirement. Even unintentional, non-reckless, non-negligent damage may violate this provision, a misdemeanor for first-time offenders.

¹¹⁴ See Center for Democracy & Technology, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology* 31-38 (Feb. 22, 2006) available at <http://www.cdt.org/publications/digital-search-and-seizure.pdf>.

¹¹⁵ [Heckenkamp?]

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

should be presumptively narrower, and Judges should require the sworn agent to present specific, targeted evidence, in the form of past training and experience or other documented examples, that this class of criminals is likely to hide data. Since the standard for probable cause is low, the agent may meet this higher showing more often than not, but it should not be presumptively granted as it is now.

Second, tools exist which cut against the power of the data hider. Think of these as the 21st-century equivalent of the x-ray. Files can be scanned for “signatures” which reveal characteristics about the data within without revealing the contents.¹¹⁶ A Judge could mandate the use of such tools, and if, for example, a tool concluded that a file contained nothing but music, then a further search of that file pursuant to a warrant to search for financial documents would not be allowed as outside the scope of the warrant. If the police can introduce tales of the Superuser data hider, it seems proportionate to let Magistrate Judges ask about privacy-protecting tools that may be used by the Superinvestigator.

c. For Scholars

[Scholars should avoid offensive and defensive uses of the Myth. Happily there are many good examples of how to refer to powerful computer users without falling prey to the myth; many scholars explicitly acknowledge that the effect of the Superuser depends on whether there are many or few. They refer to Superusers as outliers that can be ignored. They call for further empirical study to measure the effect of the powerful. These are all examples of ways to avoid the trap.]

3. 60/40, 80/20, or 99/1?

Over time, if the Myth of the Superuser is routinely dispelled, we can develop solution sets for problems that vary based on the percentage of Superusers in a population. For example, if 99% of the users responsible for a perceived harm are ordinary users using ordinary tools (the average Napster user circa 1998, for example) it would not make sense to pass sweeping, broadly phrased laws to strike out at the 1% of the users with Superuser abilities (the Napster user who masked her IP address before logging on).

On the other hand, if 40% of those who cause harm are Superusers (the people who release self-propagating worms, for example, probably include many experts) then problem may require addressing the question of what to do with the Superuser.

There are no hard-and-fast rules about what Superuser ratios trigger caution. In some cases, 80/20 may signify enough Superuser activity to justify scrutiny and regulation; in other cases, 80/20 may still mean that the problem can adequately be addressed if the 80% who are ordinary users can somehow be deterred.

Another important consideration is the Superusers’ collective impact. If only 5% of the actors are Superusers, but those 5% cause such wide-ranging harm that they are the majority of the problem, perhaps the deference I advocate need not be given. If anonymous and pseudonymous e-mail is sent by tens of thousands of people, but a few

¹¹⁶ [Salgado?]

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

hundred have created tools and services that amount for most of the anonymous e-mail sent, then a solution to the “problem” of anonymous e-mail may need to tackle that 5%.¹¹⁷

B. Additional Difficulties

1. Script Kiddism

A sound objection to the claim that the Superuser is a Myth is that Superusers can empower ordinary users to exert greater power, by creating easy-to-use and easy-to-find tools that automate Superuser-like skills. In computer security circles, ordinary users empowered to act like Superusers are known as “script kiddies,” an often-derogatory term that belittles the lack of skill and the age of the stereotypical kiddie.¹¹⁸

Often, the Myth of the Script Kiddie is exactly the same type of mistake as the Myth of the Superuser. Just because Superusers can sometimes create easy-to-use tools, does not mean that they can always do so nor does it mean that they have the incentive to do so.

Some online attackers battle vigorous countermeasure-creating communities. Even when a Superuser attacker breaches a defense, the countermeasure group will patch the hole, disabling the attack. In those cases, there may not be time to package automated tools.

For example, the spam filtering community is an aggressive, active countermeasure group. They constantly update sophisticated signatures that can be used to identify past spam messages and that can even evaluate whether a never-before-seen message has the tell-tale signs of spam. Given the speed with which this community can respond, I doubt that an automated spam-sending tool would avoid these filters for long. Although Superuser spammers could constantly update publicly-distributed tools in an escalating arms race, they are unlikely to have the incentive to do so on a scale that would empower average users who want to get into the spamming business. More likely, Superuser spammers spend their time developing techniques to evade the latest counter-measure, and sell their services to would-be advertisers.

Nevertheless, some Superuser skills can and have been automated into tools for the ordinary user. As an early example, in 1995, Dan Farmer and Wietse Venema created a tool that would conduct a series of previously known scans and attacks against a target computer to check for vulnerabilities. They called the tool SATAN for “Security Administrator Tool for Authorizing Networks.” The tool was easy-to-install, ubiquitously available, and featured a point-and-click interface. The authors contended that they were releasing the tool to the public to encourage better security by empowering

¹¹⁷ Even in such a case, there are ways to target only the Superusers and pass laws that have no effect on the ordinary anonymous e-mailer. I address these strategies in Part IV.B.2, *infra*.

¹¹⁸ [Cite].

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

network security administrators to scan their own networks. Of course, nothing in the tool prevented people from using SATAN to attack networks other than their own.¹¹⁹

Thus, sometimes the Myth of the Script Kiddie is not a myth. Returning to my original definitions, when Superusers have empowered script kiddies, there is no Myth of the Superuser. If a potentially large population can effect great change—even if that power is obtained through a tool instead of through skill and study—then this greatly affects the need for a response and changes the type of responses that may be appropriate. Many online copyright struggles fit this profile. Ordinary users have been empowered to download millions of copyrighted songs and movies through tools like Napster, Gnutella, and Kazaa, and services like the Pirate’s Bay. Broad regulatory responses may be justified in these cases, because the threat of great power is no myth—it is reality.¹²⁰

For conflicts that currently lack script kiddies: what can be done to stop Superusers from empowering ordinary users? Given a conflict in which Superusers are few and have not yet automated their power—the earlier spam example or DRM lockpicking may fit this model—how do you prevent Superusers from creating tools to empower ordinary users? There are two imperfect solutions: incentive wedges and prohibitions on tool distribution.

a. Incentive Wedges

Randy Picker has proposed what he terms, “Incentive Wedges,” to keep ordinary users apart from the Superusers who can break DRM’s digital locks.¹²¹ He proposes that digital music and movies that are sold to ordinary users be encoded with data that uniquely ties each copy to its purchaser. He speculates that a user will be less likely to give a copy of his music to a Superuser DRM lock picker if he knows that his identity is bound up with the copy. Likewise, the ordinary user is less likely to use software reputed to break DRM in order to upload files to a peer-to-peer network in that situation.¹²² The authors of the Darknet paper make a very similar recommendation.¹²³

¹¹⁹ Another famous script kiddie tool is SubSeven. A computer infected with the SubSeven backdoor could be controlled by any Internet user with a related program called the SubSeven client. SubSeven gained notoriety for two main reasons: First, many Internet worms installed SubSeven onto every vulnerable computer they could find. This meant that the installed base of SubSeven-infected computers was high. Second, the software used to control a SubSeven-infected computer is notably easy to use. The program looks like any other Windows program—some versions even have a shiny logo—with ominous buttons entitled “delete,” “see desktop,” “webcam,” and “get recorded passwords,” all intended to act from a distance to control the infected computer.

¹²⁰ I am not intending to comment on the legal status of these networks, as this has been covered in great depth elsewhere. [String cite.] I am simply commenting on the role of the Superuser in the debate over peer-to-peer sharing networks. If we take the position that peer-to-peer technologies subject their creators to copyright infringement liability, then the Myth of the Superuser should not stop regulators from taking action to stem the powerful users of these networks.

¹²¹ Randal C. Picker, *Mistrust-Based Digital Rights Management*, (forthcoming 2006).

¹²² *Id.*

¹²³ Biddle et al. *supra note 90* at xx.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

Although there are some difficulties with this suggestion, it holds promise for other Superuser conflicts. By severing the incentives of the ordinary user from the Superuser, the problem of script kiddism can be reduced.

[Picker has identified one type of Incentive Wedge: put the ordinary user at risk of detection or liability and he is less likely to collaborate with the Superuser. Risk in this case is created through technology, but it could also be created by law.]

b. Prohibitions on Distribution

Another way to deal with script kiddies is to make it a crime to distribute tools and technologies that empower people to do harmful things. Two prominent examples exist in computer crime law: the DMCA and the anti-Wiretapping Device provisions of 18 U.S.C. § 2512. Both criminalize the manufacture and distribution of tools perceived to cause specific harms—the circumvention of DRM under the DMCA and eavesdropping and wiretapping under section 2512.

Taking these two examples as models for other tool distribution prohibitions, an interesting question should be asked: Why is the DMCA so controversial while section 2512 is not? The obvious reason is that section 2512 is rarely used to prosecute anybody. Then again, the DMCA is also rarely prosecuted,¹²⁴ although civil litigation (and especially) the threat of civil litigation is fairly prevalent.¹²⁵ Another possible reason for the difference in perception is that section 2512 pre-dated the spread of the Internet and the concomitant rise of online civil liberties groups like EFF, CDT, and EPIC. The odds are good that if section 2512 did not exist and were proposed today, it would meet fierce opposition.

There is another possible reason why the two laws are regarded differently: the DMCA targets technology that has many potential beneficial, non-illegal uses—many law-abiding citizens would like to make copies of their DVDs and software to back them up, time-and-space shift, make commentary, or for other potential fair uses.

There are fewer reasons why the general public needs to use a tool “primarily useful for the surreptitious interception of communications.”¹²⁶ People in messy divorces and whistle-blowers may need to surreptitiously record audio conversations; network systems administrators and concerned parents may need to monitor computer communications, but all of these people can use general-purpose tools (tiny digital voice recorders and packet sniffers) that don’t fall within the prohibition. The law seems narrowly targeted at

¹²⁴ [Sklyarov; Mod-chip cases.]

¹²⁵ [Lexmark. Chilling Effects website.]

¹²⁶ 18 U.S.C. § 2512.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

things like transmitters hidden in desk calculators¹²⁷ and (possibly) some forms of spyware.¹²⁸

This is another path for keeping Superusers and script kiddies apart. If one characteristic of a tool makes it especially pernicious and that one characteristic is unlikely to be useful for widespread, non-pernicious use, perhaps a narrow law can be written criminalizing the creation or distribution of that tool.

To take one example, encryption experts speak about a particularly pernicious form of attack called the “man-in-the-middle” attack.¹²⁹ The basic idea is that if an attacker can insert himself between two communicating parties at the right moment in the conversation, he can convince both parties that they are having a secure conversation with one another, while in reality the man in the middle can see everything. Setting up this kind of attack is definitely beyond the ken of the average user. However, it is conceivable that an easy-to-use tool could empower ordinary users to perform the attack. As far as I know, no such tool exists. If man-in-the-middle software begins to proliferate, a narrowly-written law that targets the creation of such tools could help keep Superusers apart from script kiddies, probably without intruding on a tool the general public legitimately needs to use.¹³⁰

A final, not insignificant objection to this recommendation is that the creation of code is like speech, in fact, some courts have held it to be protectable First Amendment expression.¹³¹ Although a full response to this objection is outside the scope of this

¹²⁷ U.S. v. Biro, 143 F.3d 1421, 142? (11th Cir. 1998) (affirming convictions under section 2512 for sale of electronic transmitters hidden in three-prong wall plugs, pens, and calculators).

¹²⁸ U.S. Dep’t of Justice, *Creator and Four Users of LoverSpy Program Indicted*, <http://www.usdoj.gov/criminal/cybercrime/perezIndict.htm> (visited July 17, 2006) (announcing indictment relating to spyware designed to masquerade as an electronic greeting card). I helped investigate the LoverSpy case when I worked for the Department of Justice.

¹²⁹ Something from Schneier’s textbook?

¹³⁰ Of course, the law should be written narrowly, to avoid criminalizing cryptography research, defined broadly to include useful tinkering of the Superuser working on his own. One way to distinguish research from script kiddism is by focusing on the “ease of use” of the final product. A “proof-of-concept” tool created by a researcher is unlikely to have a polished interface, or a one-click, automated operation. Research tools are meant to be designed quickly and are meant to be used by the creator or by other experts. It may be possible to point to a moment in time in the “finishing” process where the focus shifts from proof-of-concept to empowering the masses. To err on the side of caution, the prohibition should be well beyond that line.

¹³¹ [Crypto case out of the 6th (?) Circuit.]

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

Article, even if some code is expressive speech, the types of tools described here seem to embody enough conduct elements as to not run afoul of the First Amendment.¹³²

2. Dealing with Actual Superusers

Although my main purpose is to argue for better fact-finding and a presumption that Legislators legislate as if the Superuser does not exist, sometimes the Superuser *does* exist, and does create great harm. I am not arguing that Superusers should never be regulated or pursued. Many of the most notorious and costly computer crimes throughout the short history of computer crime have been committed by people with above-average skill.¹³³ Nevertheless, given the checkered history of the search for Superusers—the overbroad laws that have ensnared non-Superuser innocents, the amount of money and time and effort that has been consumed that could have been used to find many more non-Superuser criminals, and the spotty track record of law enforcement successes—the hunt for the Superuser should be narrowed and restricted.

If a new, significant Superuser threat emerges that demands a legislative response, how should responsible policymakers structure new laws, surveillance/search capabilities, and resources to avoid past mistakes? I offer four recommendations: (1) draft narrow prohibitions that target what makes a Superuser a Superuser; (2) favor tools, dollars, and manpower over new surveillance and search capabilities; (3) constantly revisit the battlefield to see if conditions have changed; and (4) in many cases, do nothing and wait to see if the technologists can save us instead.

a. Crafting a Superuser-Specific Prohibition

As I have argued, the chief evil of past efforts to criminalize the acts of the Superuser has been the tendency to broaden the elements of the crime, and in particular the conduct elements, in an attempt to cover metaphor-busting, impossible-to-predict future acts. If legislators choose to regulate the Superuser, in order to avoid the overbreadth trap they should focus on prohibiting that which separates the Superuser from the rest of us: his power over technology. Rather than broaden conduct elements to make them more vague and expansive, tighten them to require the use of power—or even, the use of unusual power—in the commission of the crime.

Take for example, the Superuser-induced phrase, “access without authorization,” in 18 U.S.C. § 1030. Access without authorization is a prerequisite to several different computer crimes in section 1030, most notably the damage-to-a-computer crimes of subsection 1030(a)(5).

As Orin Kerr has argued,¹³⁴ this phrase, in all of its vague glory, has been construed to apply to many quite-ordinary acts that do not seem to amount to “computer hacking,” and in many cases, seem unworthy of criminal or even civil sanction. A travel agency was

¹³² For a much more detailed treatment of this topic, see Eugene Volokh, *Crime-Facilitating Speech*, 57 Stan. L. Rev. 1095 (2005).

¹³³ [Mitnick; Yahoo DoS; Morris Worm.]

¹³⁴ Orin Kerr, *Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003).

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

found to access without authorization their competitor's public website because it "scraped" information from the site using a computer program instead of a web browser.¹³⁵ A man accessed without authorization his employer's computer that he had permission to access, because he was sending files to a competitor for whom he planned to work in the near future.¹³⁶

Kerr proposes an amendment that makes the phrase more Superuser-aware. He argues that an act should not be ruled to have been done "without authorization" under section 1030 unless the actor "circumvented code-based restrictions on computer privileges."¹³⁷ In other words, no act falls within the prohibition without meeting 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. Visits to public websites would probably not suffice, and breaking an employment contract certainly would not.

As another example, consider again the DMCA. The DMCA prohibits the circumvention of digital locks (DRM) used to limit access to works protected by Copyright.¹³⁸ One reason the law has been criticized since before its passage is that the law places no serious limits on how sophisticated the DRM must be before it gains the backing of the prohibition. Although the law extends only to DRM that "effectively controls access" to a copyright-protected work, that phrase is defined elsewhere in the statute 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."¹³⁹ Courts have interpreted this phrase to place almost no restrictions on the level of sophistication required. Under this definition, scrambling techniques that are trivial to unscramble, maybe even techniques that can be circumvented on accident, satisfy the low hurdle for protection.¹⁴⁰

¹³⁵ EF Cultural Travel BV v. Explorica, 274 F.3d 577, 583 (1st Cir. 2001).

¹³⁶ Int'l Airport Centers v. Citrin, __ F.3d __ (7th Cir. 2006).

¹³⁷ *Supra note* 136 at 1656.

¹³⁸ 17 U.S.C. § 1201(a)(1).

¹³⁹ 17 U.S.C. § 1201(a)(3).

¹⁴⁰ As an example, when Dmitri Sklyarov was charged in July 2001 for creating software that could be used to copy electronic books from Adobe Corporation's eBook reader, the criminal complaint revealed that one of the technologies protecting the eBook reader was BPTe_Rot13.¹⁴⁰ Rot13 is a scrambling algorithm used sometimes by schoolchildren. It involves replacing every letter in a message with the letter that comes 13 places later in the alphabet. Every A is replaced with an N, every B with an M, etc. In other words, this is a trivial encryption method.

Granted, it is not clear from the criminal complaint that the Government asserted that Rot13 is the technology that "effectively controls access," although it would appear to fall within the broad definition. If the DMCA lends legal force to a prohibition on Rot13 unscrambling (or even the unscrambling of more complex but still simple algorithms), then the DMCA deserves the ridicule it often receives.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

The DMCA is thus an example of a law that can be more narrowly rewritten to tackle the Superuser so as not to cast an overbroad net on ordinary users. For example, “effectively controls access” can be amended to require digital locks that pass a particular threshold of complexity. Perhaps this could be defined as encryption algorithms that have been peer-reviewed and use a key-length of 64 bits or the equivalent. 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 endless copyright infringement) with ensuring that average, ordinary users aren’t prosecuted for doing ordinary things or investigated for months before the pall of suspicion passes over them. The idea is to craft laws that are limited to preventing the type of power that Superusers wield.

The danger with defining criminal acts with respect to the technical power wielded is the guilt by association problem described above. If lawmakers create prohibitions defined by a person’s technical sophistication and power, then other elements of those prohibitions should protect researchers, students, security professionals, etc., 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.¹⁴¹

Likewise, the mens rea elements can separate the researcher from the powerful Superuser attacker. However, as I discuss in Part III.B.3, this is not usually a useful limiting strategy since mens rea elements are investigated late in the lifecycle of a case.

b. Surveillance and Search

Because the Superuser criminal is often skilled at evading detection and identification, catching the Superuser requires new surveillance laws or new exceptions to pre-existing laws. Lawmakers should be wary about the speed with which they enact these new laws and the scope with which they expand them.

For example, consider the amendment made in the USA PATRIOT Act to extend Pen Register and Trap and Trace surveillance authority to any “dialing, routing, addressing, and signaling” information associated with an electronic communication. Before this change, the authority applied only to “numbers dialed.”¹⁴² The principal purpose of this amendment was to extend Pen Register/Trap and Trace authority (which is relatively easy for the police to obtain) to the non-content portions of Internet communications—IP addresses, e-mail addresses, etc. But the phrase chosen—“dialing, routing, addressing, and signaling”—is expansive.

¹⁴¹ Cite DMCA.

¹⁴² DOJ argued at the time that this amendment did not change the statute’s scope, since they had convinced Judges prior to the amendment to grant these orders for Internet communications. They characterized the amendment as a clarifying amendment to enshrine current law. See Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1196-97.

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

The new language applies to any medium—satellite, WiFi, microwave, optical—and any encoding scheme that can currently be imagined. DOJ pushed for broad language because of a fear that any narrower language would be easy to evade.¹⁴³ In other words, they invoked the Superuser. We should not tie the authority to today’s technology, they argued, because we want the law to adapt to whatever communications technology is used by criminals tomorrow.

A more measured response would have been to draft a narrow amendment that extended the Pen Register/Trap and Trace authority only to Internet communications or (even more narrowly) Internet communications over wires. Then, whenever a new communications medium became popular with criminals or the general public, Congress would have been forced to debate the proper level of privacy to afford the new medium. Now, at least for non-content information, that decision has been made once and for all.

[But why should surveillance laws expand at such a slow, methodical pace? If Superusers exist, even if there aren’t many of them, how else are we to find them except through new legal authorities? As I have stated, the police can use surveillance laws that are expanded to address the most sophisticated among us to monitor all of us. Pre-empting a slow debate about the unique particular structure of each new medium by choosing a low-privacy option once and for all raises the floor of our privacy expectations without sufficient care or debate.]

If surveillance and search laws are written narrowly, then how can law enforcement track down Superuser criminals? I recommend more resources instead of new authorities. More agents, better training, and better tools will probably help in the hunt for the Superuser as much as broader surveillance laws. Granted, more resources could also have the indirect effect of intruding into the private lives of more innocent people (by giving the FBI the luxury of pursuing more leads, for example), but this seems less likely and less troubling to me than the certainty that new laws will permit wider dragnets that pull in more innocent people.

c. Constantly Revisit the Problem

As conditions change and the tools and power available to users evolve, the fact-finding I advocate should continue as an ongoing process. If legislators heed my advice and refuse to expand a law or broaden a surveillance practice to address a hypothetical Superuser, they should periodically revisit the question to see if the battlefield has shifted. Conversely, if a broad new prohibition is written to address a widespread power, the lawmakers should pay attention to significant new countermeasures or other developments that confine the power to smaller segments of the population. When the power recedes, the laws should be rolled back.

So too should scholars engaged in debates continually reassess how much skill a particular harmful act requires. Major breakthroughs in technology can upend the entire

¹⁴³ *See id.*

DRAFT: PLEASE DO NOT CITE OR REDISTRIBUTE
August 31, 2006: As Submitted to TPRC

analysis. Finally, judges scrutinizing search warrants should continuously ask for the latest updates about how technology has made detection easier or more difficult.

d. Do Nothing and Wait for the Technologists

The prevalence and power of the Superuser can shift as the technical battle wages. When an Operating System provider patches a significant number of old vulnerabilities; a record company develops a significantly more advanced DRM technology; or a researcher develops a breakthrough in decryption technology, the pressing need for new laws may subside. Sometimes yesterday's crisis seems quaint in the face of new, ground-shifting technology. Lawmakers should often react to the problem of the Superuser by doing nothing. Wait to see if new technologies or the operation of the market will solve the problem without law.

CONCLUSION

There are two versions of my argument: a weak form and a strong form. Although I believe both to be true, I have sought to prove only the weak form in this paper. I have attempted to prove that debates about online conflict are often built upon an impoverished empirical foundation because of the Superuser. We are given and given to sweeping generalizations about powerful users when we would be better served by statistics and expert advice about the sources of trouble and harm. I am hoping to shore up our empirical foundation by questioning the Myth of the Superuser and by calling for a more nuanced discussion about the facts of the battles before us. In short, I am trying to change the debate, but not necessarily to take sides.

The stronger form of the argument is that there are very few Superusers in most online conflicts, and that the few Superusers do not cause a disproportionate amount of the harm. Although I expect this is true for most online conflicts, I have not yet taken the empirical steps to show this with rigor. Even if the stronger form of the argument is untrue in some cases—perhaps Superusers do cause most of the harm in virus writing—we would be better able to react and assess the tradeoffs of potential solutions if we knew this fact with greater certainty.

In the course of writing this article, I had an enlightening e-mail exchange with a technologist at the Electronic Frontier Foundation. He took exception to my "hostility" to the idea that all DRM is inherently flawed. Early in our exchange, he pointed to the Darknet paper as proof of this hypothesis. By the end of the exchange, although he had not changed my mind and I don't think I had changed his, instead of citing one reference to the Darknet paper, he provided paragraphs and paragraphs of history about the evolution of DRM and DRM-crackers and analyses about why DRM is doomed to failure. It occurred to me that this exchange exemplified the result that I seek. Sweeping away the rhetorical short-cut that the Myth of the Superuser represents brings us closer to understanding the true nature of the problems we are trying to solve.