Printed in U.S.A.
Vol. 107, No. 2

HACKING SPEECH: INFORMATIONAL SPEECH AND THE FIRST AMENDMENT

Andrea M. Matwyshyn

ABSTRACT—The Supreme Court has never articulated the extent of First Amendment protection for instructional or "informational" speech—factual speech that may be repurposed for crime. As technology advances and traditional modes of speech become intertwined with code speech, crafting a doctrine that expressly addresses the First Amendment limits of protection for informational speech becomes pressing. Using the case study of "vulnerability speech"—speech that identifies a potentially critical flaw in a technological system but may indirectly facilitate criminality—this Article proposes a four-part "repurposed speech scale" for crafting the outer boundaries of First Amendment protection for informational speech.

AUTHOR—Assistant Professor of Legal Studies and Business Ethics at the University of Pennsylvania's Wharton School; faculty affiliate of the Center for Technology, Innovation and Competition at the University of Pennsylvania School of Law; and Affiliate Scholar of the Center for Internet and Society at Stanford Law School. She thanks Marty Redish for his decades of "1337" legal scholarship, his tireless commitment to hacking the minds of his students, and his comments and critiques of this work. She also thanks Ian Brown, Jennifer Granick, Jennifer E. Hill, Mike Hintze, Marcia Hoffman, Nien-he Hsieh, Orin Kerr, Bronwen Matthews, Helen Nissenbaum, Paul Ohm, Deborah Pierce, Jon Pincus, Chuck Rose, Hope Rosen, Alka Tandan, Marcia Tiersky, Eugene Volokh, Lindsey Wegrzyn, Kevin Werbach, and Kim Zetter for their thoughtful critiques and criticisms. Any mistakes herein are her own. She can be reached at amatwysh@wharton.upenn.edu.

Our cases have not yet considered whether, and if so to what extent, the First Amendment protects . . . instructional speech.

—Justice John Paul Stevens[†]

INTRODUCTION

This is the story of Jack and the jackpot. In July 2010, an information security researcher named Barnaby Jack[1] caused an Automated Teller Machine (ATM) to spew pretend money[2] into an uproariously cheering audience of "hackers"[3] at DEF CON, a leading information security

[†] Statement of Justice Stevens in *Stewart v. McCoy*, 537 U.S. 993, 995 (2002), regarding the Court's refusal to review a Ninth Circuit decision reversing a conviction under an Arizona law that prohibits advising gang members on gang policy and practices. No Supreme Court case squarely addresses instructional speech.

[1] Barnaby Jack, *Jackpotting Automated Teller Machines Redux*, DEF CON, http://www.defcon.org/html/defcon-18/dc-18-speakers.html#Jack (last visited Mar. 21, 2013).

[2] Jack's presentation at DEF CON was his second of the week; he had previously presented this research at Black Hat 2010 a few days prior. *See* Robert McMillan, *Barnaby Jack Hits ATM Jackpot at Black Hat*, COMPUTERWORLD (July 28, 2010, 9:08 PM), http://www.computerworld.com/s/article/9179844/Barnaby_Jack_hits_ATM_jackpot_at_Black_Hat (describing Jack's presentation at Black Hat, which he repeated at DEF CON). Word of the dramatic nature of the presentation had spread, and the audience at DEF CON was filled with hundreds of attendees. *See* Dean Takahashi, *Researcher Shows How to Hack ATMs with "Dillinger" Tool*, VENTUREBEAT (July 28, 2010, 2:27 PM), http://venturebeat.com/2010/07/28/researcher-shows-how-to-hack-atms-with-dillinger-tool/.

[3] The audience included a motley assortment of individuals, including the author of this Article, who attends the conference annually. For a description of information security conference attendees, see, for example, *Official DEF CON FAQ v0.95*, DEF CON, http://www.defcon.org/html/links/dc-faq/dc-faq.html (last visited Mar. 21, 2013).

conference held annually in Las Vegas.[4] Although his ability to succeed in this "exploit"—or act of information security compromise—demonstrated his skill as a security researcher, his ability to control the ATM in this manner existed not only because of his hacking prowess, but also because of flaws in the way that the software running the ATM had been coded.[5] Step by step, Jack demonstrated the vulnerabilities in the build of the machine to the audience. He also highlighted critical problems in physical security around the machine: the ATM was available for purchase and delivery on eBay, a key circumstance that had facilitated the months of code analysis (from the comfort of Jack's own home) and had led him to select that particular ATM.[6]

This is also the story of the First Amendment and instructional speech, or, what Professor Martin Redish has termed "informational" speech[7]—speech that conveys factual information that can be repurposed for crime.[8] The idea of someone explaining how to cause a potentially improperly programmed ATM to eject—or, as the industry calls it, "jackpot"[9]—money will viscerally strike many legal academics and judges as speech that brazenly advocates criminality. They will question the social value of such speech and ask whether it treads into the territory of unprotected speech under the First Amendment. Meanwhile, this initial legal instinct sits diametrically opposed to the dominant thinking in the burgeoning information security research community: the default assumption among seasoned researchers and ingénues alike is one of full First Amendment protection for this type of speech. In reality, the doctrinal First Amendment truth lies somewhere in the middle: the law is unclear.[10] The Supreme Court has never expressly addressed the doctrinal question.

Building on the work of Professor Redish, this Article grapples with the legally undertheorized but critically important doctrinal tensions around the First Amendment status of informational speech—a doctrinal question

---

[4] *See generally* DEF CON, http://www.defcon.org (last visited Mar. 21, 2013) (discussing the conferences and archiving information about them).

[5] *See* McMillan, *supra* note 2.

[6] *See* Mike Cassidy, *Hacker Breaks Into ATMs for Good, Not Evil*, PHYS.ORG (Sept. 16, 2010), http://phys.org/news203844123.html.

[7] *See* Martin H. Redish, *Unlawful Advocacy and Free Speech Theory: Rethinking the Lessons of the McCarthy Era*, 73 U. CIN. L. REV. 9, 80 (2004).

[8] In other words, informational speech does not refer to mere voicing of opinion that may, for example, contain violent hyperbole. Instead, it refers to speech that is potentially directly usable by a criminal.

[9] *See, e.g.*, Henry Schwarz, *Black Hatted*, HENRY SCHWARZ'S ATM & EFT-POS SECURITY BLOG, http://henryschwarz.blogspot.com/2012/06/black-hatted.html (last visited Mar. 21, 2013).

[10] Meanwhile, a reasonable consumer potentially might be most interested in whether the vulnerability was ever fixed. (It was.) Ryan Naraine, *ATM Makers Patch Black Hat Cash-Dispensing Flaw*, ZDNET (Aug. 23, 2010, 12:14 AM), http://www.zdnet.com/blog/security/atm-makers-patch-black-hat-cash-dispensing-flaw/7210.

flagged but left unresolved by the Supreme Court.[11] Specifically, this Article examines the broader dynamics of informational speech through a case study of what I term "vulnerability speech"—informational speech that identifies a potentially critical flaw in a technological system or product but also indirectly potentially facilitates criminality. Technology advancements further complicate the doctrinal tensions the Court has left unresolved regarding informational speech. Informational speech, such as vulnerability speech, now blends traditional modes of informational speech with a second bundle of doctrinally unresolved First Amendment issues—those around code speech.[12]

This Article offers a novel technology-neutral First Amendment paradigm for addressing informational speech—a "repurposed speech scale." Part I introduces the doctrinal tensions around informational speech as it intermingles with the doctrinal tensions around code speech. Part II explores the case study of vulnerability speech and offers a construction of value for informational speech built around possible positive incidental effects and scarcity. Part III introduces the "repurposed speech scale," an approach that builds on prior First Amendment scholarship, in particular the work of Professor Martin Redish. The repurposed speech scale creates a protected space for discussion of social policy matters, even when risks of significant nonspeech harms may result. Thus, it offers a contextual approach to informational speech that assists in determining whether a speaker's intent is salutary or criminal: it requires reasonable care from the speaker in his selection of time, place, and manner for his speech in order for his speech to be deemed fully protected under the First Amendment.[13] Specifically, the scale identifies four factors: (1) the asserted goal of the speaker in his speech, (2) the reputation of the forum, (3) the scarcity of the

[11] *See* Stewart v. McCoy, 537 U.S. 993, 995 (2002) (Stevens, J.) (statement regarding the Court's refusal to review a Ninth Circuit decision reversing a conviction under an Arizona law that prohibits advising gang members on gang policy and practices).

[12] Vulnerability speech is not the only technology-driven context that highlights the open First Amendment questions around informational speech. For example, informational speech questions similarly arise with respect to instructions and code for 3D printers that enable the printers to create restricted or regulated products such as guns and other weapons. *See, e.g.*, Andy Greenberg, *Here's What It Looks Like to Fire a (Partly) 3D-Printed Gun (Video)*, FORBES (Dec. 3, 2012, 8:30 AM), http://www.forbes.com/sites/andygreenberg/2012/12/03/heres-what-it-looks-like-to-fire-a-partly-3d-printed-gun-video/. Instructional speech questions also arise with respect to postings made by speakers in forums such as 4chan known to be frequented by hacktivists. *See, e.g.*, Annemarie Dooling, *4chan 101: Message Boards for Non-Hacktivists*, HUFFINGTON POST (Sept. 2, 2011, 5:36 PM), http://www.huffingtonpost.com/2011/09/02/4chan-101-message-boards-_n_943909.html.

[13] For a discussion of contextual integrity, see generally HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010), urging a broader approach to privacy that considers norms in various social contexts, rather than the contemporary approach of merely distinguishing between the public and private spheres. A finding of protection for speech under the First Amendment can immunize the speaker from criminal prosecution or civil suit. *See, e.g.*, Herceg v. Hustler Magazine, Inc., 814 F.2d 1017, 1020 (5th Cir. 1987).

information contributed, and (4) the extent of risk mitigation by the speaker. Finally, applying the repurposed speech scale to the case study of vulnerability speech, two scenarios are likely to trigger the need for the scale. First, the repurposed speech scale would, for example, circumscribe any congressional attempts to prohibit vulnerability disclosure in its entirety. Second, the repurposed speech scale offers methodology for an intent analysis in cases where vulnerability researchers or resellers are charged with criminal offenses, including aiding and abetting acts of computer intrusion, conspiracy, economic espionage, and possibly treason.

I. INFORMATIONAL SPEECH 2.0: UNLAWFUL ADVOCACY PLUS CODE SPEECH

Let us return to Jack and the jackpot. Jack's presentation clearly falls into the category of informational speech: the knowledge Jack shared could, in theory, be repurposed by criminals. To complicate matters further, in the course of Jack's DEF CON presentation, Jack not only verbally explained each step of the compromise of the ATM, but he also displayed written information and used code as part of both the demonstration and the compromise itself.[14] As Jack's ATM-vulnerability disclosure demonstrates, today's informational speech intermingles both code and noncode elements into a single context. Yet, Jack's speech also happened not only in real time, but also in various "time-shifted"[15] multimedia formats: Jack's presentation was extensively covered by press and is still available for viewing on YouTube years later.[16] In other words, in order to craft a successful First Amendment approach to informational speech, the precedent and theory around unlawful advocacy and informational speech must be informed by the precedent and theory around code speech and vice versa. Yet, both of these areas of First Amendment jurisprudence suffer from doctrinal holes.

A. Unlawful Advocacy and Informational Speech

Although noted First Amendment scholars have voiced doubts regarding the doctrinal fit,[17] instructional or informational speech presumptively arises as a doctrinal branch of incitement and unlawful advocacy.[18] The exact doctrinal contours around informational speech

---

[14] *See* McMillan, *supra* note 2.

[15] The term "time-shifting" arises out of the intellectual property context and means a delayed use. *See, e.g.*, Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 421 (1984).

[16] *E.g.*, SecurityWeek, *SecurityWeek.Com—Barnaby Jack Hacks ATM at Black Hat*, YOUTUBE (July 28, 2010), http://www.youtube.com/watch?v=qwMuMSPW3bU.

[17] *See, e.g.*, Redish, *supra* note 7, at 89–93; Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1185–92 (2005).

[18] For a discussion of incitement, see, for example, *Hess v. Indiana*, 414 U.S. 105, 107–08 (1973) (per curiam), which explains that "[w]e'll take the fucking street later" does not constitute incitement

remain a mystery, however; the Supreme Court has never directly addressed instructional or informational speech and has declined to review the issue when an opportunity has arisen.[19] Also, while some lower courts have already considered the issue,[20] an analysis of these decisions does not provide clear guidance.

Perhaps the most notorious case in this legal space is *Rice v. Paladin Enterprises, Inc.*[21] In *Rice*, the Fourth Circuit refused to use the First Amendment as a shield to protect a publisher from a suit in tort filed by the survivors of three individuals murdered by a contract killer who used the publisher's books to plan and carry out the killings.[22] The publisher, Paladin, argued that the books were protected by the First Amendment.[23] Paladin stipulated that although it had no specific knowledge that the killer planned to commit a crime, it knew while publishing, marketing, and distributing the two books that the publications would be used by criminals to commit murder and that this use was consistent with its intent.[24]

In contrast to *Rice*, in another situation involving wrongful death, sits *Herceg v. Hustler Magazine, Inc.*, where the Fifth Circuit shielded *Hustler Magazine* from liability in connection with a suit by the mother of a reader who had died during an act of autoerotic asphyxiation after reading a

through an imminent threat under the three-part test developed by the Supreme Court in *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam). According to Professor Kent Greenawalt, the test's language appears to require "a serious evil, a substantial likelihood that speech will cause the evil, and a close temporal nexus between speech and evil." Kent Greenawalt, *Speech and Crime*, 5 AM. BAR FOUND. RES. J. 645, 696 (1980).

[19] Stewart v. McCoy, 537 U.S. 993, 995 (2002) (Stevens, J.); *see also, e.g.*, United States v. Featherston, 461 F.2d 1119, 1121, 1123 (5th Cir.) (applying the clear and present danger test to convict black militants for teaching explosive assembly in preparation for "the coming revolution"), *cert. denied*, 409 U.S. 991 (1972).

[20] For example, in most circuits, instructions regarding tax evasion are usually deemed by courts to constitute unprotected speech, providing grounds for a speaker's conviction on grounds of aiding and abetting tax fraud. *See, e.g.*, United States v. Dahlstrom, 713 F.2d 1423, 1428 (9th Cir. 1983) (holding that tax evasion instructions must rise to the level of incitement under *Brandenburg* to constitute aiding and abetting); United States v. Buttorff, 572 F.2d 619, 624 (8th Cir. 1978) (finding that describing how to cheat on taxes is incitement, disregarding the time-sensitivity factor identified in other case law). Similarly, in *United States v. Barnett*, the Ninth Circuit upheld the conviction of a defendant who sold drug-making instructions through a mail exchange. Despite never having personal contact with the principal, furnishing instructions was sufficient to make the defendant criminally responsible for aiding and abetting. 667 F.2d 835, 842 (9th Cir. 1982).

[21] 128 F.3d 233 (4th Cir. 1997). Professor Redish argues that the case was wrongly decided. *See* Redish, *supra* note 7, at 65–66, 93.

[22] 128 F.3d at 267.

[23] *See id.* at 241–43.

[24] This stipulation may have single-handedly proven fatal to Paladin's case. Redish argues that *Rice* was wrongly decided and that the court's concern appeared to a significant part to have been the manual's purely persuasive value. "Thus, by parsing the Fourth Circuit's opinion in *Rice*, one can see that improper persuasional concerns, rather than the communication of otherwise publicly inaccessible information, underlay the court's conclusion that the manual was to be denied First Amendment protection." Redish, *supra* note 7, at 93.

detailed description of its charms in the periodical.[25] However, unlike in *Rice*, intent was not stipulated and the court noted the presence of meaningful cautionary language in the article, language that warned readers not to attempt the practice and therefore potentially signaled lack of advocacy of the practice.[26] Although an intent analysis may offer a modicum of guidance in distinguishing these cases, much doctrinal uncertainty remains with respect to informational speech and its First Amendment status.

Scholarship is similarly divided on the question of protection for instructional speech, as well as the appropriateness of using incitement analysis in instructional speech cases. Professor Thomas Emerson has argued that advice and persuasion is protected, but instructions or preparations would not be.[27] Meanwhile, Professor Laurence Tribe has stated that "law need not treat differently the crime of one man who sells a bomb to terrorists and that of another who publishes an instruction manual for terrorists on how to build their own bombs out of old Volkswagen parts."[28] Professor Eugene Volokh, on the other hand, has argued that these instructional speech cases—which he terms "crime-facilitating speech"[29]—"are not incitement cases" because the speech is not persuading hearers to commit bad acts; it simply gives people information that assists in criminality.[30] Specifically, he argues that:

> [C]rime-facilitating speech ought to be constitutionally protected unless (1) it's said to a person or a small group of people when the speaker knows *these few listeners are likely to use the information for criminal purposes*, (2) it's within one of the few classes of *speech that has almost no noncriminal value*, or (3) it can cause *extraordinarily serious harm* (on the order of a nuclear attack or a plague) even when it's also valuable for lawful purposes.[31]

Perhaps the most developed treatment of instructional or informational speech appears in the work of Professor Martin Redish. Redish argues that

---

[25] 814 F.2d 1017, 1021 (5th Cir. 1987) (finding First Amendment protection for—and thus no criminal or civil liability in connection with—the publication of an article detailing the practice of autoerotic asphyxiation, despite the reader's death).

[26] Hustler's meaningful cautionary language stated: "Hustler emphasizes the often-fatal dangers of the practice of 'auto-erotic asphyxia,' and recommends that readers seeking unique forms of sexual release DO NOT ATTEMPT this method. The facts are presented here solely for an educational purpose." *Id.* at 1018.

[27] *See* THOMAS I. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 75 (1970).

[28] LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 837 (2d ed. 1988).

[29] Volokh defines crime-facilitating speech as: "(1) any communication that, (2) intentionally or not, (3) conveys information that (4) makes it easier or safer for some listeners or readers (a) to commit crimes, torts, acts of war (or other acts by foreign nations that would be crimes if done by individuals), or suicide, or (b) to get away with committing such acts." Volokh, *supra* note 17, at 1103 (footnote omitted).

[30] *See id.* at 1102.

[31] *Id.* at 1106.

none of the currently available doctrinal conceptual approaches[32] to unlawful advocacy, "standing alone, provides an adequate resolution of the competing interests in free expression and national security."[33] Conceptually, Redish carves out informational speech from unlawful advocacy, and in doing so, he offers a novel framework for informational speech.[34] He highlights both the social importance of a speech-protective approach to informational speech, but he adopts a more balanced approach than Volokh, recognizing possible national security risks from unfettered informational speech in certain contexts.

Redish explains informational speech and how its treatment should differ from that applied to unlawful advocacy:

> Although as a traditional matter unlawful advocacy is assumed to seek to persuade others to take illegal actions, on occasion speech that does no more than inform can reasonably be thought to proximately lead to unlawful conduct.
>
> . . . .

---

[32] Redish identifies four fundamental approaches to unlawful advocacy regulation. First, "definitional absolutism," which protects under the banner of the First Amendment all activity that is "included within the definition of 'speech,' as opposed to non-expressive conduct." Second, "categorical balancing," which balances various interests by determining specific categories of activity that are worthy of protection prior to a legislative or judicial challenge. Third, "deferential balancing," where a reviewing court generally defers to legislative or executive determinations regarding whether particular expression advocating unlawful conduct will be regulated, suppressed, or punished. Fourth, "speech-protective balancing," which attempts to "balance competing interests in maintaining free and open expression on the one hand and in assuring security and preventing violence on the other hand," while including a "strong presumption in favor of the constitutional protection of speech." Redish, *supra* note 7, at 17.

[33] *Id.* at 16. Redish argues that "[t]he best solution to the unlawful advocacy conundrum is found in an approach that selectively synthesizes elements of several of the previously proffered scholarly theories of unlawful advocacy regulation, to form a radically different conceptual and doctrinal approach to the unlawful advocacy conundrum." *Id.* at 17.

[34] Redish proposes a "selective categorization" model that "would pick and choose among the various models, depending upon an *ex ante* categorical division among different groupings of factual circumstances." *Id.* at 80. He recognizes four groupings: "(1) 'confined' unlawful advocacy; (2) 'unconfined' unlawful advocacy; (3) speech-acts; and (4) informational speech." *Id.* Redish also explains that:

> [D]irectly coercive expression has no place under the First Amendment's umbrella. . . . On a purely definitional level, we have already seen that the mere fact that words are used does not automatically render those words protected expression. . . . [O]ne can imagine a case where an individual issues the command, "fire," to a firing squad poised to commit an execution. In this case, the particular word used does make a difference, yet again it is difficult to characterize this verbal effort as expression. The word is so intertwined with the action that it effectively becomes part of the action. Similarly, where words are used in a directly coercive manner, as in the case of blackmail or threats, it is appropriate to exclude those superficially expressive acts from the definition of speech.
>
> . . . .
>
> . . . [A]t some point, a synthesis of the speaker's intent and the listener's reaction of fear or coercion will necessarily justify application of a coercive speech exception.

Id. at 85–87.

> . . . [I]t makes sense to treat informational expression . . . differently from the way purely persuasive advocacy is treated. . . . The focus should, for the most part, be on a synthesis of four factors: (1) the likelihood that communication of the information will lead to an illegal activity; (2) the potential harmfulness of the behavior to which the information is likely to lead; (3) the extent to which the public already possesses access to the information through alternative means; and (4) the potential value to the public of the revealed information. Each consideration is to be deemed a necessary condition to justify the removal of constitutional protection.[35]

It is this theoretical building block upon which the sections that follow rest.[36] But due to technological advancements, Redish's insightful approach begins to strain. As the following Parts of this Article demonstrate, mixed-media or technology-assisted informational speech—particularly vulnerability speech—exacerbates the preexisting First Amendment doctrinal holes concerning informational speech. They are now compounded with another set of doctrinal First Amendment holes—those around code speech.

B. Informational Speech Meets Code Speech

As the example of Jack's informational speech in the introduction demonstrates, new media—including the Internet and computer code—have become intertwined with the informational speech of the past. Therefore, it becomes essential to inform any successful doctrinal approach to informational speech with an understanding of the dynamics of new media. In other words, an informational speech framework should strive to

---

[35] *Id.* at 89–90. Redish further explains the third factor: "Indeed, it is arguable that the third criterion should be deemed satisfied only when the information is contained in documents classified as secret by the government." *Id.* at 90. Regarding the fourth factor, Redish concedes that:

> Inclusion of the fourth factor—the potential value of the revealed information—is admittedly a highly risky strategy. Normally, it is not for the courts to gradate First Amendment protection o[n] the basis of their subjective judgments of the value of regulated speech. In the context of informational expression regulation, however, inclusion of the value consideration should serve only as a one-way ratchet: [a court considers the fourth factor] if, and only if, application of the first three factors would lead to the validation of speech regulation. In such a situation, reference to the fourth factor could serve as a possible safety valve to constitutionally insulate the expression from suppression. For example, in the so-called Pentagon Papers case, . . . absent this fourth factor a court could conceivably have held the suppression unconstitutional, solely on the grounds that the previously classified information concerning the history of American involvement in Vietnam had potentially significant value to the public's assessment of a major political controversy.

Id. at 91.

[36] Building from Redish's approach to informational speech, Part III highlights conceptual challenges that arise for dual-purpose informational speech such as vulnerability speech. It melds Redish's four factors with key elements of the *O'Brien* and *Corley/Vartuli* tests to generate a framework perhaps more attuned to the mixed communication media reality of today that includes code speech. The framework balances stimulating debate on matters of public concern in novel, esoteric knowledge spaces on the one hand, and limiting the weaponization of that speech to protect national security interests on the other. For a discussion of the *O'Brien* test, see *infra* note 72 and accompanying text.

be simultaneously technology neutral but informed by the unique dynamics of new technologies. As such, the doctrinal tensions around unlawful advocacy and informational speech must be blended with the doctrinal tensions around code speech. Vulnerability speech such as Jack's and other novel technology-mediated speech contexts[37] force us to confront these existing doctrinal deficits in tandem.

In particular, two problematic First Amendment questions emerge from this doctrinal blending. First, current First Amendment doctrine lacks a coherent framework for analyzing computer code as speech in nondigital contexts. Second, assuming both code and accompanying expression are deemed potentially protected speech, no doctrinal clarity exists on the point of when this blended multimedia expression crosses the line from protected informational speech into unprotected unlawful advocacy. In particular, it is not clear how to doctrinally unpack informational speech in a context like the Internet—a context where code, i.e., the speech itself, can be used as a weapon by third parties to inflict national security harms.[38]

1. Code Speech: Lessons About Technology Neutrality.—As explained by Professor James Gibson, "[L]egal regulation of computer code raises First Amendment concerns and brings to the fore related issues of autonomy, transparency, and accountability—although the degree to which formal First Amendment protection should apply to code is a matter of much debate."[39] Although several cases have litigated the extent of First Amendment protection for code, these first-generation code speech cases have left open several vexing doctrinal holes, for example, whether code on a website should be analyzed differently from identical code written on a T-shirt.[40]

A majority of scholars and experts have argued that code is usually speech for First Amendment purposes.[41] However, some legal scholarship

---

[37] *See supra* note 12.

[38] For example, foreign governments might use zero-day exploits of the caliber of Flame, an unusually sophisticated piece of malware, to inflict significant damage on the United States' interests. For a discussion of the sophistication of Flame and similar viruses, see, for example, *Flame: Trying to Unravel the Mystery of 'Sophisticated' Spying Malware*, PBS NEWSHOUR (May 30, 2012), http://www.pbs.org/newshour/bb/science/jan-june12/theflame_05-30.html; David Goldman, *Super-Virus Flame Raises the Cyberwar Stakes*, CNN MONEY (May 30, 2012, 1:41 PM), http://money.cnn.com/2012/05/30/technology/flame-virus/index.htm; Raphael Satter, *Security Firm: New Computer Virus Prowling Mideast*, BLOOMBERGBUSINESSWEEK (Aug. 9, 2012), http://www.businessweek.com/ap/2012-08-09/kaspersky-weve-found-new-virus-linked-to-stuxnet.

[39] James Gibson, *Once and Future Copyright*, 81 NOTRE DAME L. REV. 167, 189–90 (2005).

[40] *See infra* text accompanying notes 53–56.

[41] *See, e.g.*, Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L.J. 629 (2000) (arguing that code is usually properly classified as speech for First Amendment purposes); *see also* Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L.J. 713, 720 (2000) (disagreeing with portions of Tien's analytical framework, but agreeing that computer code "that is itself part of the public dialogue" is speech covered by the First Amendment). Other contributions to the debate over the constitutional status of code include Dan L. Burk, *Patenting Speech*, 79 TEX. L.

has asserted that courts "should have adopted a more nuanced intent-based test that would consider the speaker's purpose in publishing code."[42] But scholars disagree about the appropriate contours of this protection, and some authors have questioned, in particular, the appropriateness of extending First Amendment protection to potentially malicious code: viruses[43] and exploit code.

a. Code and intellectual property harms.—A tension between intellectual property law and the First Amendment is clearly visible in the first generation of code speech cases—particularly on the point of code presented in nondigital media. In *Universal City Studios, Inc. v. Corley*,[44] the Second Circuit considered the constitutionality of the antitrafficking provisions of the Digital Millennium Copyright Act[45] under the First Amendment. The defendants, Corley and his company, 2600 Enterprises, Inc., a hacker enthusiast publication, challenged the DMCA in connection with an injunction barring Corley from publishing DeCSS, a program released by a Norwegian teenager and two unidentified individuals, which circumvented copy protection on DVDs.[46]

REV. 99 (2000); Ryan Christopher Fox, Comment, *Old Law and New Technology: The Problem of Computer Code and the First Amendment*, 49 UCLA L. REV. 871 (2002); and R. Polk Wagner, Note, *The Medium Is the Mistake: The Law of Software for the First Amendment*, 51 STAN. L. REV. 387, 398 (1999) (arguing for a more context-based approach to First Amendment protection of code, which "asks whether the regulation [of computer code] is intended to suppress free expression").

[42] Recent Case, Universal City Studios, Inc. v. Corley, *273 F.3d 429 (2d Cir. 2001)*, 115 HARV. L. REV. 2042, 2045 (2002); *see also* Orin S. Kerr, *Are We Overprotecting Code?: Thoughts on First-Generation Internet Law*, 57 WASH. & LEE L. REV. 1287, 1290–93 (2000) (arguing that computer code should be analyzed based on what it says, not what it is, and that treating all code as speech covered by the First Amendment merely because it consists of language is overinclusive).

[43] *See, e.g.*, David McGowan, *From Social Friction to Social Meaning: What Expressive Uses of Code Tell Us About Free Speech*, 64 OHIO ST. L.J. 1515, 1519 (2003); Robert Plotkin, *Fighting Keywords: Translating the First Amendment to Protect Software Speech*, 2003 U. ILL. J.L. TECH. & POL'Y 329, 348–51.

[44] 273 F.3d 429 (2d Cir. 2001). For a discussion of *Corley*, see, for example, Joseph P. Bauer, *Copyright and the First Amendment: Comrades, Combatants, or Uneasy Allies?*, 67 WASH. & LEE L. REV. 831, 861 n.153 (2010), and Greg Lastowka, *Decoding Cyberproperty*, 40 IND. L. REV. 23, 67–70 (2007); see also Greg Lastowka, *Digital Attribution: Copyright and the Right to Credit*, 87 B.U. L. REV. 41, 45–46 (2007), discussing the Digital Millennium Copyright Act, which the defendants challenged on constitutional grounds in *Corley*.

[45] Digital Millennium Copyright Act, 17 U.S.C. § 1201(a)(2), (b)(1) (2006). The DMCA targets not only the circumvention of digital walls such as encryption, "but also anyone who would *traffic* in a technology primarily designed to circumvent a digital wall." *Corley*, 273 F.3d at 435.

[46] Corley wanted to make DeCSS available for download on his website, which was a corollary to his print publication. *Corley*, 273 F.3d. at 434–35. In November 1999, Corley posted an article about the movie industry, DVDs, and DeCSS to his website. *Id.* at 439. The article detailed how CSS, the encryption technology used in DVDs, was cracked and the legal battles around DeCSS, the program that cracked it. *Id.* At the end of the article, Corley posted and linked to a copy of the object and source code of DeCSS. At trial, he argued that writing a story about DeCSS without including the code would have been "analogous to printing a story about a picture and not printing the picture." *Id.* The lower court "entered a permanent injunction barring Corley from posting DeCSS on his web site or from

The Second Circuit explained that "[c]ommunication does not lose constitutional protection as 'speech' simply because it is expressed in the language of computer code."[47] Nevertheless, the court asserted that intermediate and not strict scrutiny was appropriate for code speech because computer code can achieve results with only a "momentary intercession of human action," which could be "as limited and instantaneous as a single click of a mouse."[48] Consequently, the court reasoned that computer code should receive a lower level of First Amendment protection than ordinary speech because of this "functionality" argument—the ability of code to "instantly cause a computer to accomplish tasks . . . [means that] functionality is really a proxy for effects or harm."[49] Ultimately upholding the injunctions, the Second Circuit reached for an analogy from physical space, implicitly comparing the posting and linking of DeCSS to a bookstore that chooses to sell and distribute obscene materials.[50] As Professor Dan Burk has eloquently described, courts' struggles to find parallels in physical space for code has manifested itself in the confusion over regulating computer code in different formats, resulting

knowingly linking via a hyperlink to any other web site containing DeCSS" and rejected arguments that the injunction violated the First Amendment protections. *Id.* at 436.

[47] *Id.* at 445.

[48] *Id.* at 451.

[49] *Id.* (quoting Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 331 (S.D.N.Y. 2000)) (internal quotation marks omitted).

[50] *See id.* at 457. Ultimately, the Second Circuit upheld the antitrafficking provisions of the DMCA, framing the questions around the protectability of code as issues best reserved for Congress because they implicate public policy choices. *Id.* at 452.

A second case to undertake this analysis similarly upheld an injunction against a poster of DeCSS. In *DVD Copy Control Ass'n, Inc. v. Bunner*, the California Supreme Court analyzed the appropriateness of injunctive relief in connection with DeCSS software under California's version of the Uniform Trade Secrets Act. 75 P.3d 1, 9 (Cal. 2003). The lower court had concluded that the plaintiff was likely to prevail on the merits and would suffer irreparable harm without injunctive relief. *Id.* at 9–10. The lower court concluded that the CSS technology contained protectable trade secrets, derived independent economic value from its secrecy, and reasonable efforts had been made to sustain its secrecy. Further, the court determined that the author of DeCSS had obtained these trade secrets through reverse engineering processes in violation of a license agreement, constituting acquisition through improper means. *Id.*

The California Supreme Court, despite acknowledging that code is entitled to First Amendment protection, also upheld both the preliminary injunction against Bunner's First Amendment challenges and the permanent injunction, provided that the injunction was warranted under California's trade secret law. *Id.* at 19–20. The court found no basis in the First Amendment to prevent such injunctions. *Id.* Bunner claimed he had posted DeCSS on his website because "it would enable Linux users to use and enjoy DVDs available for purchase or rental in video stores and make Linux more attractive and viable to consumers." *Id.* at 7 (internal quotation marks omitted). As the court in *Bunner* noted, trade secret law also seeks to promote and maintain commercial standards, a significant governmental interest. *Id.* at 12. The court asserted that "'[t]he mere fact that' Bunner 'claims an expressive . . . purpose does not give [him] a First Amendment right to 'appropriat[e] to [himself] the harvest of those who have sown.'" *Id.* at 14 (alterations in original) (quoting S.F. Arts & Athletics, Inc. v. U.S. Olympic Comm., 483 U.S. 522, 541 (1987)).

in different treatment for symbols printed in hardcopy and symbols in machine-readable media.[51] Professor Radin has also commented on "the anomalous dual treatment of computer programs in intellectual property law. Computer programs are both text and machine. They are text when considered as code statements, they are machines when considered as devices for accomplishing a task."[52]

This confusion from intellectual property law regarding whether code is text or machine has also filtered into—or at least is implicit in—First Amendment jurisprudence. For example, during the time that DeCSS was being shared in the wild on the Internet, Copyleft, a small New Jersey-based company, created T-shirts that were emblazoned with the source code for DeCSS.[53] The advertisements for the shirts stated that the shirts functioned as a way to "[s]how [their] disapproval of the DVD CCA"[54] and as a way to make a protest statement against the DMCA. However, shortly after the shirts were referenced at trial during the *Corley* case, Copyleft was added as a defendant in the litigation.[55] Unsurprisingly, the DVD CCA claimed that the shirts constituted "every bit as much of a theft of the trade secrets as was the posting on websites which was enjoined by the courts."[56] Although a preliminary injunction was issued, it was lifted on appeal. Thus, the First Amendment issues that these T-shirts raised about mixed media—in this case, the cotton reproduction of cryptography code—were never resolved, despite being echoed in the later code "trafficking" cases. And, as Part I.B.2 will explain, these questions are now resurfacing in the context of vulnerability speech.

b. Code "trafficking".—A second strand of code speech cases—what might be termed the "code trafficking" cases—left open the question of when software crosses the line from an expressive communication into a regulable commodity. This second strand of code speech cases highlights

---

[51] *See, e.g.*, Burk, *supra* note 41, at 105. Professor Burk has insightfully argued that an "imminent collapse" looms for "the carefully drawn constitutional balance between the Intellectual Property Clause and the Free Speech Clause." *Id.* at 102.

[52] Margaret Jane Radin, Lecture, *Online Standardization and the Integration of Text and Machine*, 70 FORDHAM L. REV. 1125, 1143 (2002).

[53] Four dollars from the sale of each T-shirt was donated to the Electronic Frontier Foundation in order to defray the cost of defending the individuals and organizations who were named in the DeCSS lawsuits instituted by the DVD industry. *See* Sara Crasson, Note, *Are DeCSS T-Shirts Dirty Laundry?: Wearable, Non-Executable Computer Code as Protected Speech*, 15 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 169, 193 (2004). However, not all content is protected by default under the First Amendment, particularly when copyright or trademark infringement is involved. Professor Burk correctly cautions that despite substantial overlap, "the scope of expression in copyright and the scope of expression in free speech are not coextensive. . . . [T]he First Amendment clearly protects some types of expression that the copyright statute does not cover." Burk, *supra* note 41, at 126.

[54] Crasson, *supra* note 53 (alteration in original).

[55] *Id.* at 194; *see* Farhad Manjoo, *Court to Address DeCSS T-Shirt*, WIRED (Aug. 2, 2000), http://www.wired.com/science/discoveries/news/2000/08/37941.

[56] Manjoo, *supra* note 55.

the challenge of distinguishing between regulating speech and regulating potentially hazardous materials, a tension that was presciently identified by Professor Dan Farber:

> In tomorrow's world, however, the two categories [of digital speech and digital products] will probably be more difficult to distinguish, a change that is already underway. Expressive commodities—economically valuable information transmissions—often can be seen as either commodities or expression. Speech regulations may no longer seem so sharply unlike commercial regulations, as the boundary between commerce and speech erodes.[57]

As Professor Dan Burk reminds us, while the First Amendment may protect a report describing a scientist's research, it is doubtful that the First Amendment prohibits the regulation of the underlying research materials. The government can restrict the movement and dissemination of such materials if, for example, they contain "organisms that may prove pathogenic or ecologically destructive."[58]

It was precisely this type of tension that led the Second Circuit to differentiate its own decision in *Corley* from its decision in *Commodity Futures Trading Commission v. Vartuli*.[59] In *Vartuli*, a software program called Recurrence was sold by its creators for the purpose of telling users when to buy or sell futures contracts through analyzing currency futures market transactions.[60] The Commodity Futures Trading Commission charged the defendants with violating federal law for, among other things, failing to register as commodity trading advisors in connection with their distribution of the software.[61] The defendants argued that the software was protected speech and that the registration requirement was an impermissible prior restraint.[62] The Second Circuit rejected the defendants' constitutional claim and stated that "in the form it was sold and marketed by the defendants," it did not generate speech protected by the First

---

[57] Daniel A. Farber, *Expressive Commerce in Cyberspace: Public Goods, Network Effects, and Free Speech*, 16 GA. ST. U. L. REV. 789, 789–90 (2000) (footnote omitted).

[58] Burk, *supra* note 41, at 111. The cryptography-algorithm code trafficking cases highlight this tension. For example, the source code for Pretty Good Privacy (PGP), an e-mail encryption software package, is currently available for purchase as a hardcover book on Amazon. *See PGP: Source Code and Internals [Hardcover]*, AMAZON.COM, http://www.amazon.com/PGP-Internals-Philip-R-Zimmermann/dp/0262240394/ref=sr_1_1?ie=UTF8&s=books&qid=1292276076&sr=8-1 (last visited Mar. 21, 2013). Yet PGP's creator, Phil Zimmermann, was investigated for several years because of the code's publication online, which was alleged to violate U.S. export restrictions regarding cryptographic software. *See Philip Zimmermann: Creator of PGP and Zfone*, PHILZIMMERMANN.COM, https://www.philzimmermann.com/EN/background/ (last visited Mar. 21, 2013).

[59] 228 F.3d 94 (2d Cir. 2000).

[60] *See id.* at 98–99.

[61] *See id.* at 100.

[62] *See id.* at 109.

Amendment.[63] In particular, the Second Circuit highlighted that instead of trying to generate debate over matters of public interest connected to commodities trading, the software encouraged users to adhere to its recommendations blindly, without second-guessing or analyzing.[64] In other words, the court asked whether the distribution of the software knowingly furthered an illegal enterprise or sought to stimulate debate—the same question at issue in an analysis of informational speech under the First Amendment.

Meanwhile, the Ninth Circuit, in *Bernstein v. United States Department of Justice*,[65] addressed a challenge to restrictions on the export of cryptography from the United States. Bernstein, a student at the University of California, Berkeley, sought to publish a paper and associated source code on an encryption system he had authored.[66] The Ninth Circuit ruled that Bernstein's source code constituted speech protected by the First Amendment and that the restrictions on its publication were unconstitutional.[67] However, in concluding comments, the Ninth Circuit was clear in highlighting that the holding was a narrow one[68] and that the court did not hold that all software is expressive speech[69] for purposes of the First Amendment. In the words of the court, "We do not hold that all software is expressive. Much of it surely is not."[70]

Meanwhile, in *Karn v. United States Department of State*, the U.S. District Court for the District of Columbia decided a case involving export

---

[63] *Id.* at 111.

[64] *See id.*

[65] 176 F.3d 1132 (9th Cir. 1999).

[66] *See id.* at 1135–36.

[67] *See id.* at 1145.

[68] *See id.*

[69] Despite the Ninth Circuit's hesitation in deeming all code expressive, an argument exists that code functions at least as a diary would for its authors. For example, a leading information security researcher recently tweeted, "It is a curious sensation, revisiting code you wrote long ago. Not unlike having mental conversations with your younger self." Dan Kaminsky, *@dakami*, TWITTER (July 15, 2012, 6:26 PM), https://twitter.com/dakami/status/224676355877502976.

[70] *Bernstein*, 176 F.3d at 1145. Similarly, in *Junger v. Daley*, the Sixth Circuit considered the request of a law professor to post encryption source code on his website in connection with demonstrating the functionality of the code to his students. 209 F.3d 481, 483 (6th Cir. 2000). He submitted three applications to the Commerce Department asking for a determination with respect to whether export restrictions covered the code. *Id.* The Export Administration found that the first chapter of Professor Junger's textbook was an allowable unlicensed export, but asserted that the export of the book in electronic form would require a license if the text contained the software. *See id.* at 484. Junger then filed a facial challenge to the export regulations on First Amendment grounds. *Id.* While remanding the case to the district court for consideration of Junger's constitutional challenge to the regulations, the Sixth Circuit deemed source code to be protected under the First Amendment, stating that "[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment." *Id.* at 485. However, the court went on to say that "[w]e recognize that national security interests can outweigh the interests of protected speech and require the regulation of speech." *Id.*

control limitations on diskettes containing source code for cryptographic algorithms.[71] Unlike the Ninth and Sixth Circuits, this district court upheld the regulation of the diskettes under the *O'Brien* test,[72] reasoning it is within the power of the government to control the export of defense articles, and it furthers the significant government interest in the regulation of cryptographic products in a narrowly tailored way.[73]

Hence, cases such as *Vartuli*, *Bernstein*, and *Karn* also offer no clear guidance in determining when code is protected as speech and when code is regulable as a product. As technology has progressed, this blurring of the digital speech–digital product line has become even more complicated. In particular, today's code speech embodies the potential of both simultaneous *and* "time-shifted" harm to arise from informational speech such as Barnaby Jack's—a novel feature of today's second-generation informational speech, which blends both code and noncode elements as part of the communication.

2. Second-Generation Informational Speech: Simultaneous and "Time-Shifted" Harms.—In an exceptionally forward-looking

---

[71] 925 F. Supp. 1 (D.D.C. 1996). As Lee Tien explains:

> The oral argument in *Karn* . . . presents an example of how critics confuse the medium and the message. During the oral argument, the D.C. Circuit presented a hypothetical about AWACS planes—ordinary planes converted to perform special functions. The court hypothesized that one could place this special function into a CD-ROM containing a computer program, then display this software as text or numbers on a screen, and finally transcribe it into a book that the First Amendment would cover. The court then asked, "Does it follow that the CD-ROM that got slipped into the hardware of the airplane is speech?"
>
> This question confuses the information recorded on the CD-ROM with the package consisting of the disk and the recorded information. The correct approach must distinguish between the software as text, the form of the text, the physical medium, and running the software. . . .

Tien, *supra* note 41, at 687 (footnotes omitted).

[72] *See infra* notes 95–97 and accompanying text. The *O'Brien* test refers to the test set forth by the Supreme Court for expressive conduct in *United States v. O'Brien*, 391 U.S. 367 (1968). In *O'Brien*, the Supreme Court addressed the issue of whether a regulation prohibiting the burning of draft cards constituted a prior restraint on speech that violated the First Amendment. *Id.* at 370–72. The Court determined that "when 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms." *Id.* at 376. Consequently:

> [A] government regulation is sufficiently justified if it is within the constitutional power of the Government; if it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest.

Id. at 377. For a discussion of *O'Brien*, see, for example, Eugene Volokh, *Speech as Conduct: Generally Applicable Laws, Illegal Courses of Conduct, "Situation-Altering Utterances," and the Uncharted Zones*, 90 CORNELL L. REV. 1277, 1284 (2005) ("The distinction [between speech and conduct] . . . should be the one suggested by *United States v. O'Brien* and the other cases that distinguish content-neutral from content-based speech restrictions: Expression can generally be regulated to prevent harms that flow from its noncommunicative elements (noise, traffic obstruction, and the like), but not harms that flow from what the expression expresses.").

[73] *See Karn*, 925 F. Supp. at 11.

article, Professor Margaret Radin argued that the distinction between technological standards and legal standards is becoming progressively blurred.[74] And as Professor Radin predicted, convergence between technological and legal standards increasingly seems inevitable.[75] This inevitability is visible in the First Amendment challenges presented by second-generation informational speech. Code is increasingly simply one piece of a broader social conversation occurring across various social spaces, including various spaces mediated by technology.[76] It is precisely this dynamic—the unresolved tensions of code printed on T-shirts versus websites from *Corley* and the unresolved "dangerous" code issues raised by *Vartuli* and *Berstein* in the context of national security and criminal activity[77]—that second-generation informational speech forces us to include in a First Amendment informational speech analysis. In other words, today's informational speech presents a doubly complicated First Amendment inquiry because it frequently involves analyzing a single communication that occurs across multiple interwoven communication media simultaneously. However, perhaps counterintuitively, this mixed-media operationalization of second-generation informational speech means

[74] *See* Radin, *supra* note 52. Indeed, an insightful *Harvard Law Review* note provided the example of the instability of diminished protection for all code speech because of the inevitable human–machine convergence the future will hold. *See* Recent Case, *supra* note 42, at 2045 n.33 (providing examples of other forms of speech that, like some code, are both "speech" in the traditional sense and machine executable, such as "a Braille version of *Hamlet* [that] can be run through a machine that will read the book out loud"). Diminishing the protection for a particular person's speech simply because the speech was mediated by a code device—such as dictating a memoir or a law review article draft using Siri—should not diminish the protectability of the speech from a First Amendment standpoint.

[75] We have entered the reality where coded ideas in technological spaces can have immediate, dramatically socially disruptive consequences in physical spaces—a stolen election, a destroyed power grid, a hacked stock market, a dead patient. Vulnerability speech forces us to confront the questions of how to prop up the marketplace of ideas in a technological reality that moves at a blazing speed and, as the examples listed above show, carries the potential for enormous consequences.

[76] As Professor Jennifer Granick explains:

> [T]here are strong reasons to reject the argument that code is different, and that restrictions are therefore good policy. Code's functionality may help security as much as it hurts it and the open distribution of functional code has valuable effects for consumers, including the ability to pressure vendors for more secure products and to counteract monopolistic practices.

Jennifer Stisa Granick, *The Price of Restricting Vulnerability Publications*, INT'L J. COMM. L. & POL'Y, Spring 2005, at 1, 1.

[77] Although it may be conceptually troubling for First Amendment purposes, the United States has historically placed limitations on scientifically important speech that has presumptive value under the First Amendment but that may pose a threat to national security. For example, "the 1917 Voluntary Tender Act, which gave the Commissioner of Patents the authority to withhold certification from inventions that might harm U.S. national security, and to turn the invention over to the United States government for its own use." Laura K. Donohue, *Terrorist Speech and the Future of Free Expression*, 27 CARDOZO L. REV. 233, 274 (2005). Likewise, the "Invention Secrecy Act established a prior restraint on government employees and . . . private inventors, to prevent them from publishing inventions deemed to be 'detrimental to the national security.'" *Id.* at 275 (quoting Invention Secrecy Act of 1951, ch. 4, § 1, 66 Stat. 3). The Atomic Energy Act also imposed a prior restraint on the dissemination of nuclear energy information. *See id.* at 279.

that courts should avoid a technology-exceptionalist analysis: the code speech component of informational speech is not special in its communication of content.[78] Although on its surface, the presence of numbers in lieu of Roman characters as a component of speech may seem foreign and somehow foreboding, at the most basic level, code offers merely another embodiment of ideas. It is the execution—the time, place, and manner—of the speech where variation matters, along with the extent of negative incidental consequences of the selected method of execution of the communication.

Let us return yet again to the story of Barnaby Jack and his compromised ATM at DEF CON, which offers a paradigmatic example of second-generation informational speech. Precisely, Barnaby Jack's variant of second-generation informational speech might be termed "vulnerability speech"—expression that identifies a dangerous flaw in the structure of a system or product in order to improve security. Vulnerability speech generally involves both code and noncode components, such as writings and presentations. In other words, vulnerability speech involves a description of how and why code is malfunctioning and a demonstration of how to "break" it. Usually this description is also accompanied by new code that exploits the dangerous flaw described in order to prove its existence. To wit, it may involve speech across multiple media that is inextricably interwoven with code. A second characteristic of vulnerability speech, like other second-generation informational speech, is that it involves a situation where informational speech could result in both simultaneous and time-shifted harms. Just as the DeCSS code in *Corley*[79] was available online at any time, so Barnaby Jack's ATM compromise is still available on YouTube today.[80] Further, because a talk such as Jack's will be widely distributed and discussed across media and because any accompanying code essentially recreates a portion of his speech whenever it is run, the speaker potentially "speaks" on a continuous basis—he speaks in perpetuity, as long as the talk is available for viewing and the code

[78] In *Reno v. ACLU*, the Supreme Court refused to apply a different level of First Amendment scrutiny simply because speech happened through code instead of traditional media. 521 U.S. 844, 870 (1997). As one court explained the holding in *Reno*, "[S]peech on the internet is subject to no greater or lesser constitutional protection than speech in more traditional media." United States v. Carmichael, 326 F. Supp. 2d 1267, 1288–89 (M.D. Ala. 2004).

[79] However, perhaps more so than the defendants in *Corley*, Jack's informational speech perhaps involved a "whistleblower" component, calling attention to the risk of potential criminality that may be ongoing. *See* McMillan, *supra* note 2 (quoting Jack describing his motivation as "to spark discussion on the best ways to remediate [the ATM's security problems]"). This description, like *Corley*, however, also involved an explanatory component of how one might engage in that criminality in the future.

[80] *See, e.g.*, Security Week, *supra* note 16.

available for use. In theory, his speech could be repurposed for criminality at any point.[81]

Perhaps this "time-shifted" nature of second-generation informational speech may remind us of first-generation speech in some respects. For example, a reader may read instructions on becoming a hit man, the same way that he might watch a YouTube video about how to exploit a vulnerable ATM. However, one can argue that the possible inclusion of executable[82] code and the potentially perpetual real-time nature of second-generation informational speech may make it more akin to attending a rally, such as that in *Hess v. Indiana*,[83] or watching a recording of that rally. Thus, disagreeing with Professor Redish and Professor Volokh, I would argue that the immediacy of the risk of criminality arising out of the second-generation informational speech is, in fact, more in line with traditional incitement concerns than one might assume. However, the "immediacy" analysis from incitement doctrine—"imminent lawless action"—was certainly not crafted for the Internet age. Further, unlike *Hess*,[84] it can be argued that offering code as part of speech is more akin to handing out protest signs on wooden sticks to assist in "taking back the street"—signs that might be repurposed as bludgeoning weapons.[85] Yet, in many cases, the goals of speakers who engage in informational speech are not at all criminal: instead, frequently the goal of the informational speech is to directly contribute relevant knowledge to a social conversation on matters of national importance.

II. CONSTRUCTING THE SOCIAL VALUE OF INFORMATIONAL SPEECH: A CASE STUDY OF VULNERABILITY SPEECH

If it is indeed the case that second-generation informational speech embodies dangers that are more in line with traditional unlawful advocacy concerns than does first-generation informational speech, playing devil's advocate, one might argue that perhaps the doctrinal knots of informational speech cannot be unraveled. Is it possible that Barnaby Jack is simply a

[81] In reality, at the time he gave his presentations at Black Hat and DEF CON, he and the ATM vendor had patched the vulnerabilities and the risk of criminality was significantly mitigated. *See, e.g.*, Schwarz, *supra* note 9; *see also* Naraine, *supra* note 10 (describing the patches introduced by ATM makers to fix the flaws Jack identified).

[82] Executable code refers to code in a form that can be run by a computer, as opposed to source code, which is meant to be interpreted by a human programmer and which requires an extra step before it can be run by the machine. *See Definition of: Executable Code*, PCMAG.COM, http://www.pcmag.com/encyclopedia_term/0,1237,t=executable+code&i=42842,00.asp (last visited Mar. 21, 2013).

[83] 414 U.S. 105 (1973) (per curiam).

[84] *See id.* at 110 (Rehnquist, J., dissenting).

[85] Despite the presence of code that can be used for an improper purpose in vulnerability speech, when examining the factors identified by the lower court in *Hess* as the hallmarks of incitement, the exhortations in *Hess* can be viewed as a better fit than vulnerability speech, and yet the Supreme Court ultimately protected the expression.

wolf in sheep's clothing—a particularly cunning criminal posing as a researcher and merely claiming good intentions? Perhaps the most logical solution is simply to deem all instructional speech unprotected advocacy of criminality? Although this approach would certainly be expedient, it would nevertheless result in a highly undesirable outcome in many cases. As Professor Redish insightfully asserted,[86] the potential social value of informational speech warrants consideration, despite the messiness of this undertaking: "[T]o allow government to characterize as unprotected unlawful advocacy speech that is on its face nothing more than informational could give rise to a pervasive chilling effect on the distribution of information that is potentially valuable on a number of levels."[87]

The next section unpacks this question of the social value of informational speech. Specifically, it tries to operationalize the social value factor Professor Redish included in his framework, highlighting its complicating role. In this section, using the case study of vulnerability speech, I argue that social value of informational speech can be assessed as a combination of two factors: first, the totality of possible positive incidental effects arising from the speech, and, second, the scarcity of the contributed information.

A. Of Hit Men and Hackers: Shooting Victims Versus Shooting Messengers

While the image of Barnaby Jack's ATM shooting money into the hands of possible "hacker" malefactors is certainly a dramatic one, the more interesting part of the story for purposes of a legal analysis occurred long before Jack's high-profile demonstrations.[88] Jack and his employer at the time had delayed the presentation for a year in order to allow the ATM vendor to correct the flaws in its product.[89] By cooperating with the vendor,

---

[86] *See* Redish, *supra* note 7, at 90.

[87] *Id.*

[88] *See* Carl Franzen, *Barnaby Jack Ingeniously Hacks ATMs at Black Hat*, AOLNEWS (July 29, 2010, 11:35 AM), http://www.aolnews.com/2010/07/29/barnaby-jack-ingeniously-hacks-atms-at-black-hat-video/.

[89] In the words of one engineer at the ATM manufacturer:

> Barnaby and his colleagues had planned to present his work . . . relatively soon after we had learned of his attack, so we insisted that they delay their presentation until we had sufficient time to roll-out our patch to more ATMs. Barnaby's employer ultimately acquiesced, albeit grudgingly, and his Black Hat 2009 presentation was cancelled. Apparently this cancellation was something of a minor scandal among some Black Hat participants, who condemned his employer as cowardly caving to The Man. Of course I am biased, but I truly view his employer's decision as an example of conducting security research responsibly. . . .
>
> . . . .
>
> . . . The enormous benefit is that our ATM is now significantly more secure, because we didn't just plug the hole that Barnaby discovered, but we took our defense a thousand times further. . . .

Schwarz, *supra* note 9.

they not only assisted the company in correcting the product's information security imperfections,[90] but they also limited the likelihood that criminality would arise from Jack's informational speech. Because both sides cooperated, acknowledged the imperfections in the product, and worked to remedy them, on the day that hacker crowds bathed in fake dollar bills raining from the stage, the flaws discovered by Jack were already corrected and the risk of criminality had been minimized.[91] Consumers were a little safer as a result.

But let us imagine that a different ATM company produces machines that—without Jack's knowledge—suffer from flaws similar to those in the machines Jack compromised. Let us imagine that a criminal uses Jack's exploits and, in lieu of blaming itself for its information security inadequacies, the company demands that Jack be prosecuted for aiding and abetting the criminals. Or let us imagine that Jack failed to contact the ATM company to help patch the flaws. Instead, perhaps he chose to "drop 0-day,"[92] and he released information about the security flaws and exploit code "into the wild" on a blog whose readership likely includes information criminals. After criminality ensues (or a prosecutor deems a criminal act to have occurred), he is criminally prosecuted for aiding and abetting computer intrusion. Or let us imagine that the vulnerability was not part of an ATM but instead part of a weapons system. What happens if Jack sells or "gifts" a zero-day exploit to a private middleman or intermediary,[93] who then passes it on to a foreign government, which uses Jack's exploit to harm U.S. corporate or government interests? Should Jack be prosecuted for economic espionage or treason? Current First Amendment paradigms are ill-suited to analyzing Jack's speech in any of these scenarios. Yet, both the possible benefits and the possible risks implicated by vulnerability speech are significant.

1. Assessing Incidental Effects: Borrowing from United States v. O'Brien.—Professor Eugene Volokh observed that "many types of crime-facilitating speech have harmful uses; but they also have valuable uses, including some that may not at first be obvious. . . . This dual-use nature has implications for how crime-facilitating speech should be

[90] *See id.*

[91] As I explained in previous work on security, content owners sometimes rely on invasive digital rights management technologies that behave in the same harmful manner as malicious code used by information criminals, using the Digital Millennium Copyright Act and (weak constructions of) contractual consent as the legal basis for pushing this code onto users' machines. *See* Andrea M. Matwyshyn, *Technoconsen(t)sus*, 85 WASH. U. L. REV. 529 (2007). In the context of vulnerability speech, we find a different variation of this scenario: information security researchers use the tools of malicious hackers, but usually for the purpose of preventing harm.

[92] "Dropping 0-day" is slang for a release of a zero-day exploit.

[93] *See infra* notes 215–28 and accompanying text.

treated."[94] It is precisely this dual purpose of some—but not all—informational speech that complicates the First Amendment inquiry. Distinguishing between cases where only disproportionately negative incidental effects exist—i.e., *single-purpose* informational speech—from cases where both strong positive and negative incidental effects can exist—i.e., *dual-purpose* informational speech—facilitates a more nuanced First Amendment analysis of informational speech.

As the code speech cases evidence, courts have sometimes turned to an intermediate standard of scrutiny arising out of *United States v. O'Brien* as the basis of an analytical framework in cases involving code.[95] Similarly, in the context of asserting a common law duty to patch vulnerable code, I have relied on an analysis springing from *O'Brien*.[96] Here again in the context of informational speech, I argue that the language or at least the spirit of *O'Brien* offers key guidance. *O'Brien* highlights a critical factor that allows us to ferret out the distinction that Volokh postulated: *O'Brien* instructs courts to assess the incidental effects of the speech and whether they undermine key social systems.[97] By focusing on this incidental effects question from *O'Brien*, we can postulate this critical distinction between two types of informational speech—single-purpose informational speech and dual-purpose informational speech. In other words, *O'Brien* can potentially be read to suggest that the classification of informational speech as single purpose or dual purpose should matter in the analysis of its First Amendment protection. Single-purpose and dual-purpose informational speech result in dramatically different incidental effects.

Returning to *Rice v. Paladin*,[98] the import of this single- versus dual-purpose distinction becomes clear. In *Rice*, the informational speech at issue was decidedly single-purpose informational speech, and strongly negative incidental effects resulted: dead people. Few possible positive incidental effects can arise from a compilation of information about how to successfully commit various forms of murder. However, some informational speech—for example, a website explaining how to grow marijuana—may have both a strong positive and a negative incidental effect. For instance, in states where medical marijuana growing is permitted, this informational speech can result in positive incidental effects—it furthers the growth of a legal commodity that alleviates physical

---

[94] Volokh, *supra* note 17, at 1105.

[95] 391 U.S. 367 (1968).

[96] *See* Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 FLA. L. REV. 109, 145 (2010).

[97] *See O'Brien*, 391 U.S. at 370–71, 386; *see also* discussion *supra* note 72. As I explained previously, "Just as the Court in *O'Brien* found a vital interest in the continued functionality of the Selective Service System, [the negative effects of information security compromise] harm . . . society as a whole through undermining key social systems. . . ." Matwyshyn, *supra* note 96, at 147 (footnote omitted).

[98] Rice v. Paladin Enters., Inc., 128 F.3d 233 (4th Cir. 1997).

discomfort for some patients. Yet, if the same informational speech is used by growers seeking to sell marijuana in a jurisdiction where the product is illegal, negative incidental effects result—the illegal drug trade increases. Even conceding the possibility of illegal repurposing, this potential misuse does not negate the compelling possible positive incidental effects and possible high social value of some types of instructional speech.

2. The Social Stakes: A Tale of Two Vulnerable Systems.—Turning to our case study to apply this distinction between single- and dual-purpose informational speech, we must begin by asking whether there are possible positive incidental effects of vulnerability speech. The answer is yes. Vulnerability speech clearly falls into the dual-purpose informational speech category. Although negative incidental effects may indeed arise from vulnerability speech, vulnerability speech also has the potential for tremendous positive incidental effects: our future as a viable country may literally depend on the security improvements vulnerability speech may trigger.

The social conversation over information security—sometimes called "cybersecurity" in the context of national security issues involving the Internet[99]—is just beginning in the United States.[100] The last decade has been marked by the arrival of prevalent state data breach notification laws,[101] as well as dramatically increased press coverage of information

[99] Referring to all of information security, particularly in private sector contexts, as "cybersecurity" is technically incorrect. "Cyber" has traditionally referred to Internet-only phenomena. Information security is not solely an Internet phenomenon. Information security questions involve both computer security and physical security. They must be analyzed as a holistic enterprise relating to the systemic assessment of information risk throughout the life cycle of a piece of information—from the creation of a bit of information to its destruction. As such, information security involves concerns over physical attacks as well as Internet-facilitated attacks. As Barnaby Jack's compromise of the ATM demonstrates, many information security problems involve inadequate physical controls—such as being able to purchase an ATM for home delivery on eBay—and code. Further, as Bradley Manning's alleged copying of classified information demonstrates, information security frequently involves elements of physical security of devices and errors in computer code or settings that can be exploited regardless of whether the code is accessible through the Internet. *See* Athima Chansanchai, *WikiLeaks Fallout: Military Bans Thumb Drives*, NBCNEWS.COM, http://www.technolog.msnbc.msn.com/technology/technolog/wikileaks-fallout-military-bans-thumb-drives-125984 (last visited Mar. 21, 2013).

[100] Information security is also an increasingly lucrative business space. According to some estimates, the industry is expected to double in the next five years, to be worth over $120 billion by 2017. Tim Wilson, *Study: Cybersecurity Market to Double in Next Five Years*, DARK READING (July 6, 2012, 12:49 AM), http://www.darkreading.com/security/security-management/240003251/study-cybersecurity-market-to-double-in-next-five-years.html. As I have explained in prior scholarship, the legal issues around information security and software vulnerabilities implicate numerous interwoven questions of law arising from traditional bodies of law—contract, copyright, tort, securities regulation, corporate law, and common law duties of care, *see* Matwyshyn, *supra* note 96, at 125–45, and criminal law and the First Amendment, *see id.* at 147.

[101] For a discussion of data breach notification laws, see, for example, Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1884–85 (2011).

security issues.[102] The continued integrity of core social systems—our elections,[103] stock markets,[104] national defense,[105] hospitals,[106] drugs,[107] medical devices,[108] air traffic control systems,[109] energy grid,[110] water supplies,[111] nuclear reactors,[112] and communication grids,[113] to name just a few—all depend on the emergence of a vibrant vulnerability speech discourse in order to propel improvements in information security.[114] Each of these core social systems is increasingly dependent upon and controlled by code—code that is currently inadequately audited in many cases.[115]

---

[102] Privacy Rights Clearinghouse maintains a list of data breaches specifically to draw public attention to them. For a list of such data breaches, see, for example, *Chronology of Data Breaches: Security Breaches 2005–Present*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (last updated Mar. 22, 2013).

[103] *See infra* text accompanying notes 120–28.

[104] *See, e.g.*, Kim Zetter, *NSA to Investigate Nasdaq Hack*, WIRED THREAT LEVEL (Mar. 30, 2011, 2:33 PM), http://www.wired.com/threatlevel/2011/03/nsa-investigates-nasdaq-hack/.

[105] *See infra* text accompanying note 181.

[106] *See, e.g.*, Dan Kaplan, *Indiana University Hospital Hacked to Steal Data*, SC MAG. DATA BREACH BLOG (Feb. 1, 2012), http://www.scmagazine.com/indiana-university-hospital-hacked-to-steal-data/article/225887/.

[107] *See* Peter Murray, *No More Skipping Your Medicine—FDA Approves First Digital Pill*, FORBES (Aug. 9, 2012, 11:15 AM), http://www.forbes.com/sites/singularity/2012/08/09/no-more-skipping-your-medicine-fda-approves-first-digital-pill/.

[108] *See* Kim Carollo, *Can Your Insulin Pump Be Hacked?*, ABC NEWS MEDICAL UNIT (Apr. 10, 2012, 6:51 PM), http://abcnews.go.com/blogs/health/2012/04/10/can-your-insulin-pump-be-hacked/; Charlie Sorrel, *Scientists Demonstrate Deadly WiFi Pacemaker Hack*, WIRED GADGET LAB (Mar. 12, 2008, 6:32 AM), http://www.wired.com/gadgetlab/2008/03/scientists-demo/.

[109] *See* Heather Kelly, *Researcher: New Air Traffic Control System Is Hackable*, CNN TECH (July 26, 2012, 6:49 PM), http://www.cnn.com/2012/07/26/tech/web/air-traffic-control-security.

[110] *See infra* text accompanying notes 203–07. For example, nuclear power plants and oil companies might be attractive and potentially vulnerable targets for hackers. *See* Fernando Alfonso III, *Anonymous Hits Oil Companies, Leaks 1,000 Employee Logins*, DAILY DOT (July 16, 2012), http://www.dailydot.com/news/anonymous-big-oil-exxon-hack/ (oil companies); Andy Greenberg, *America's Hackable Backbone*, FORBES.COM (Aug. 22, 2007, 6:00 PM), http://www.forbes.com/2007/08/22/scada-hackers-infrastructure-tech-security-cx_ag_0822hack.html (nuclear power plants).

[111] *See South Houston's Water Supply Network Hacked*, INFOSEC ISLAND (Nov. 18, 2011), http://www.infosecisland.com/blogview/18244-South-Houstons-Water-Supply-Network-Hacked.html.

[112] *See* Colin Murdock, *8 Things You Won't Believe Can Be Hacked*, CRACKED.COM (Sept. 7, 2011), http://www.cracked.com/article_19412_8-things-you-wont-believe-can-be-hacked.html.

[113] *See* US-CERT, NAT'L CYBER SECURITY DIV., CONTROL SYS. SEC. PROGRAM, POTENTIAL VULNERABILITIES IN MUNICIPAL COMMUNICATIONS NETWORKS (2006), *available at* http://www.us-cert.gov/control_systems/pdf/Potential_Vulnerabilities_Municipal_Communications_Networks_v1.pdf.

[114] Yet, the very same speech that pushes this social policy conversation on information integrity forward has the potential to cause meaningful economic, democratic, and even sometimes physical harm to citizens.

[115] As the two examples that follow will illustrate, the flawed code that runs critical social systems is frequently written by companies from the private sector, a private sector that frequently appears to lack adequate legal and financial incentives to be vigilant about possible information security harms. For further discussion of duties to correct information security deficiencies, see, for example, Matwyshyn, *supra* note 96.

Software vulnerabilities continue to be a major obstacle to the creation of secure virtual and physical spaces.[116] Although engineers strive to build more secure software, systems remain vulnerable, and thousands of new vulnerabilities are discovered annually.[117] As I have explained elsewhere,[118] vulnerabilities in software programs expose consumers to information-based harms such as identity theft and loss of control of their machines.[119] However, when vulnerabilities exist in software used in critical social systems, such as elections or as part of the control mechanism for the power grid, the impact of vulnerable code can damage the lives of millions of people simultaneously in physical space.

For example, according to the Verified Voting Foundation, approximately a quarter to a third of all U.S. voters used paperless electronic voting machines in the 2012 November elections.[120] Yet, the security of those systems has been found to be sorely lacking in the past.[121]

---

[116] Vulnerabilities often arise from "incorrect memory management, poorly designed authentication mechanisms, and incorrect assumptions about user inputs." *What the Power Industry Has to Learn About Cyber Vulnerability Disclosure*, IEEE SMART GRID (Jan. 2012), http://smartgrid.ieee.org/newsletter/january-2012/479-what-the-power-industry-has-to-learn-about-cyber-vulnerability-disclosure.

[117] The government-sponsored National Vulnerability Database logs thousands of new vulnerabilities every year. *See id.* Vulnerabilities can generally be classified as issues arising from either the software design or implementation processes. Design issues generally spring from erroneous understanding of system security requirements, leading to inadequate authentication mechanisms, weak encryption ciphers, or limited software configurability. Implementation vulnerabilities are usually due to software programming mistakes, such as inappropriate memory allocation, errors implementing encryption mechanisms, or missing user-input validation. Both types of errors generally point to a broader deficit in an organization: inadequate focus on security in the development process as a whole. *See id.*

[118] *See* Matwyshyn, *supra* note 96.

[119] *See id.* at 113.

[120] *See* Jaeah Lee, *Every Vote Counts. Almost*, MOTHER JONES, July/Aug. 2012, at 33, 33; *see also* PAMELA SMITH ET AL., COUNTING VOTES 2012: A STATE BY STATE LOOK AT VOTING TECHNOLOGY PREPAREDNESS 10 (2012), *available at* http://countingvotes.org/sites/default/files/CountingVotes2012_Final_August2012.pdf (listing states with no requirement of paper authentication of electronically tabulated votes).

[121] For example, Princeton computer scientists reverse engineered the hardware of a Sequoia electronic voting machine and a corresponding memory cartridge. *See* ANDREW W. APPEL ET AL., INSECURITIES AND INACCURACIES OF THE SEQUOIA AVC ADVANTAGE 9.00H DRE VOTING MACHINE (2008), *available at* http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/voting/advantage/advantage-insecurities-redacted.pdf; *see also* Andrew W. Appel et al., *Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine*, PRINCETON U. CENTER FOR INFO. TECH. POL'Y, http://citpsite.s3-website-us-east-1.amazonaws.com/oldsite-htdocs/voting/advantage/ (last visited Mar. 21, 2013) (summarizing report and related litigation); Kelly Jackson Higgins, *E-Voting Machine Hack Steals Votes*, DARK READING (Aug. 12, 2009, 4:27 PM), http://www.darkreading.com/security/news/219200437/e-voting-machine-hack-steals-votes.html (describing the team's methodology). They then wrote an exploit that simulated an election. *See id.* In this way, they were capable of corrupting the results of the election. Microsoft Research also published a paper describing vulnerabilities in allegedly "fully-verifiable" direct-recording electronic systems that nevertheless allowed a hacker to "undetectably alter large numbers of votes." Josh Benaloh & Eric

In fact, vulnerabilities in some California voting machines were so severe that the State of California decertified these machines, banning them from electoral use,[122] and joined a false claims suit against the company that sold the machines.[123] However, in lieu of embracing audit by information security experts to ensure that their products are as secure as possible, voting technology companies have sometimes decided to resort to the courts to engage with their critics.[124] Yet, the vulnerabilities in these voting systems potentially remain extensive and underexplored.[125] In the words of one researcher, "It's much easier to steal the election, right at the electronic voting machine . . . . In many cases, we see security devices or electronic voting machines where we really have to wonder, 'Did anybody spend 60 seconds figuring out the security issues?'"[126]

Similarly, although by 2016 more than 75% of U.S. electric meters will be converted to smart meters,[127] the security of many of these devices is in doubt, and the shift to a smart grid carries with it new information security risks. Vulnerabilities in new smart grid technologies, like those in election software, have been well documented and, nevertheless, appear to

---

Lazarus, The Trash Attack: An Attack on Verifiable Voting Systems and a Simple Mitigation 1, http://research.microsoft.com/pubs/155590/The%20Trash%20Attack.pdf. Similarly, scientists at Argonne National Laboratory were able to successfully alter votes in some types of electronic voting machines by inserting a $10 component along with a $15 radio frequency device that manipulated touch screens by remote control, leaving no traceable evidence that vote tampering had occurred. Phil Rogers, *Most Security Measures Easy to Breach, Experts Say*, NBC CHI. (Jan. 7, 2011, 1:32 PM), http://www.nbcchicago.com/news/tech/argonne-laboratory-technology-security-breach-113054464.html#ixzz1Eku08Gug. The researchers believe these types of attacks are possible on "a wide variety of machines with little technical expertise." Rob Lever, *Questions Linger in US on High-Tech Voting*, PHYS.ORG (Mar. 11, 2012), http://phys.org/news/2012-03-linger-high-tech-voting.html (internal quotation mark omitted).

[122] This decertification was the result of joint efforts by information security researchers and journalists. *See* Ryan Paul, *California Voting Machine Security Tests Uncover Serious Vulnerabilities*, ARS TECHNICA (July 29, 2007, 11:35 PM), http://arstechnica.com/security/2007/07/california-voting-machine-security-tests-uncover-serious-vulnerabilities/.

[123] *CA Sues Diebold for E-Vote Machine False Claims*, RENSE.COM, http://rense.com/general57/machine.htm (last visited Mar. 21, 2013).

[124] *See, e.g.*, DOUGLAS W. JONES & BARBARA SIMONS, BROKEN BALLOTS (2012). Meanwhile, Congress painstakingly continues to debate the efficacy of requiring audit trails in voting machines. A bill proposed to require paper-ballot audit died but was subsequently reintroduced and is now in committee. *See H.R.5816—Voter Confidence and Increased Accessibility Act of 2011*, OPENCONGRESS, http://www.opencongress.org/bill/112-h5816/show (last visited Mar. 21, 2013).

[125] *See* Diego Aranha, Univ. of Brasilia, *Software Vulnerabilities in the Brazilian Voting Machine*, USENIX, https://www.usenix.org/conference/evtwote12/title-tbd (last visited Mar. 21, 2013).

[126] Rogers, *supra* note 121 (quoting Roger Johnston of Argonne National Laboratory). In the 2012 election, the hacktivist collective Anonymous made allegations of attempted electronic-voting-machine manipulation in Ohio and their role in preventing the success of these efforts. *See* Natasha Lennard, *Did Anonymous Stop Rove from Stealing the Election?*, SALON (Nov. 20, 2012, 7:54 AM), http://www.salon.com/2012/11/20/did_anonymous_stop_rove_stealing_the_election/.

[127] The smart grid market is surging. According to some estimates, the smart grid market currently stands at approximately $34 billion per year. *Smart Grid Market Projected at $33 Billion*, DVIRC (June 6, 2012), http://www.dvirc.org/smart-grid-market-projected-at-33-billion.

persist.[128] One veteran security expert explained it as follows: "The smart grid is a lot of different things, but, at it's core, will be a lot of embedded devices, each with a network stack to communicate with each other . . . . [The smart grid] is taking this read-only medium, from a consumer standpoint, and making it a read-write."[129] Because of this shift, the importance of minimizing security vulnerabilities in the smart grid is stark.[130] Another researcher who studies supervisory control and data acquisition (SCADA) issues highlights that public debate on smart grid vulnerability is urgent:

> Unless we wake up and realize what we're doing, there is 100% certainty of total catastrophic failure of the entire power infrastructure within 3 years . . . . How governments and utilities are blindly merging the power grid with the internet, and effectively without any protection, is insanity at its finest."[131]

As this build-out of the smart grid continues, the public debate over its desirability necessitates an assessment of the smart grid's information security—an assessment that can only occur through vulnerability speech.[132]

When information security researchers expose flaws in code, their vulnerability speech highlights ways that systems can be attacked by malefactors. But in doing so they trigger critical debate around information security, and ideally, the vulnerable systems become strengthened as a result of the speech. Thus, security researchers and their vulnerability speech perform an essential function in the information ecosystem: they frequently keep us all safe(r). Just as one of the most important functions of reputable newspapers is to run checks on the facts they present in their articles, so too security researchers are the "fact-checkers" of the information technology ecosystem. They ensure that products and systems function honestly—as advertised, as expected, and with maximum safety

---

[128] *See What the Power Industry Has to Learn About Cyber Vulnerability Disclosure*, *supra* note 116.

[129] Robert Lemos, *Smart-Grid Firms Need Security Education*, SECURITYFOCUS (Mar. 24, 2009), http://www.securityfocus.com/brief/932 (quoting Joshua Pennell, CEO of IOActive).

[130] *See* Press Release, Take Back Your Power, Hacking Expert David Chalk Joins Urgent Call to Halt Smart Grid (Apr. 12, 2012), *available at* http://takebackyourpower.net/wp-content/uploads/2012/04/Smart-Grid-Cybersecurity-Press-Release-12Apr2012.pdf. As explained by one expert, "We're in a state of crisis . . . . The front door is open and there is no lock to be had. There is not a power meter or device on the grid that is protected from hacking—if not already infected—with some sort of trojan horse that can cause the grid to be shut down or completely annihilated." *Id.* (quoting David Chalk).

[131] *Id.* (quoting David Chalk).

[132] Some local governments recognize this public concern and offer their citizens ways to opt out of the smart metering program or have instituted moratoriums on its further expansion. California, Maine, Vermont, Louisiana, Michigan, Connecticut, Quebec, the U.K., and the Netherlands currently offer opt outs. In the United States, moratoriums have been enforced in several regions, including the counties of Santa Cruz and Marin. *See id.*

for the good of the entire information ecosystem.[133] They are also the front line in addressing what I have elsewhere termed an information security "Red Queen Effect"—a constant arms race between criminals and defenders where innovation is required simply to maintain the status quo in information security.[134] In other words, vulnerability speech is a clear example of dual-purpose informational speech with strong possible positive incidental effects and thus possible high social value for society.

Having elaborated on the positive incidental effects prong of determining "high social value" informational speech, let us next turn to the question of information scarcity and its implications for a construction of a definition of "high social value" informational speech.

B. Information Scarcity: Of Harbingers and Harassment

Not all information is equally available in society. Frequently, the most useful information for purposes of a reasoned analysis of public policy is information that is not readily accessible: it is sometimes held by only a small number of experts. Dynamics around some forms of informational speech reflect this information scarcity problem. In other words, sometimes the most socially useful informational speech may also be highly esoteric and limited in availability.

1. Lessons from Information Valuation.—As trade secret law[135] and database valuation practices[136] demonstrate, the potential value of information is driven by its scarcity, not by its prevalence.[137] Similarly, the existence of whistleblower laws[138] reflects an attempt to solve an

---

[133] Another metaphor for information security researchers might be one of whistleblowers. Indeed, many information security researchers would categorize themselves in this manner. For a discussion of the various overlapping constructions of information disclosure in technology contexts, see, for example, Patricia L. Bellia, *WikiLeaks and the Institutional Framework for National Security Disclosures*, 121 YALE L.J. 1448, 1526 (2012).

[134] *See* Andrea M. Matwyshyn, *Penetrating the Zombie Collective: Spam as an International Security Issue*, 3 SCRIPTED 370, 385 (2006), *available at* http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/matwyshyn.asp#3.2.

[135] Trade secrets lose their value if publicly shared. *See, e.g.*, UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 536, 538 (2005) (defining a "trade secret" as information that "derives independent economic value . . . from not being generally known").

[136] For a discussion of database and other intangible asset valuation, see, for example, Robert F. Reilly, *Intangible Asset Valuation, Damages, and Transfer Price Analyses in the Health Care Industry*, J. HEALTH CARE FIN., Spring 2010, at 24, 25–27.

[137] It is a basic precept of information economics that scarcity drives information value. *See, e.g.*, Keith Aoki, *Authors, Inventors and Trademark Owners: Private Intellectual Property and the Public Domain PART I*, 18 COLUM.-VLA J.L. & ARTS 1, 71 (1993) ("[I]nformation is scar[c]e and such scarcity creates or destroys value.").

[138] Under Dodd–Frank, a law with representative whistleblower provisions, whistleblowers who provide information that leads to a successful SEC enforcement action may receive 10%–30% of the monetary sanctions if more than $1 million is collected. *See* 15 U.S.C. § 78u-6(b)(1) (2006). For a discussion of whistleblower laws, see, for example, Robert P. Brooks, *Understanding Key New*

information scarcity problem. In instances where informational speech exposes the speaker to risk of criminal prosecution or civil suit, many speakers will assess whether the personal risk is warranted and decide against contributing their knowledge to public debate. However, when the knowledge held by these speakers represents a scarce commodity, perhaps the product of years of professional training and expertise, the loss of their contribution to the public debate is particularly unfortunate and sometimes simply not replicable from other sources: the information their speech would have contained might not be available from any other speaker. In other words, the scarcity of particular informational speech demonstrating expertise may make it "high social value" speech.

This idea of placing a thumb on the legal scale for expertise is not new. In perhaps a somewhat parallel manner, courts frequently look to experts to guide the determination of complicated disputes.[139] Here, it can be argued that because society benefits greatly from experts' speech, risk buffers as part of an "expert-friendly" informational speech model should be crafted to incentivize experts to share their esoteric knowledge pro bono, particularly when that knowledge implicates policy issues of social importance.

2. The Pernicious Persistence of Security Through Obscurity.—Turning to our case study of vulnerability speech, the knowledge held by elite information security researchers is particularly scarce. Talent deficits in the information security space abound, and the top information security practitioners are in constant demand,[140] commanding six-figure salaries.[141] In fact, the scarcity of expertise in information security likely provides a partial explanation for why widespread information vulnerability persists in our society.[142]

For example, public companies have long been confused about securities law reporting obligations and whether severe data breaches and

Employment Regulations, *in* ROBERT P. BROOKS, COMPLYING WITH EMPLOYMENT REGULATIONS (2012), *available at* 2012 WL 3279181.

[139] For example, courts frequently turn to medical doctors to testify regarding medical issues during trial and offer professional opinions based on the doctor's expertise. For a discussion of expert testimony generally, see, for example, Brian R. Gallini, *To Serve and Protect?: Officers as Expert Witnesses in Federal Drug Prosecutions*, 19 GEO. MASON L. REV. 363 (2012).

[140] *See, e.g.*, Gordon Smith, *Skills Deficit Leaving IT Security Jobs Unfilled*, SILICON REPUBLIC (Nov. 11, 2010), http://www.siliconrepublic.com/strategy/item/18903-skills-deficit-leaving-it-s.

[141] *See, e.g.*, Fahmida Y. Rashid, *IT Security Salaries Expected to Grow 4.5% in 2012*, EWEEK (Nov. 16, 2011), http://www.eweek.com/c/a/Security/IT-Security-Salaries-Expected-to-Grow-45-in-2012-166496/.

[142] *Cf.* Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 181–82 (2005) (describing the ineffectiveness of the "security through obscurity" strategy followed by some data intensive firms, in which the firms do not disclose or otherwise foster dialogue about security risks they face).

security vulnerabilities constitute material reportable events.[143] Yet, despite this obvious confusion, the SEC issued no direct guidance on the topic until 2011[144]—guidance that the SEC asserts is currently not being followed with adequate rigor.[145] Similarly, despite ample evidence of pervasive neglect of information security in both the public and private sector since the early 2000s, the legal community has been painfully slow in understanding the importance of information security.[146]

Indeed, many companies perceive financial incentives to exist in both failing to invest in adequate information security and then attempting to hide the existence of security vulnerabilities.[147] As explained by both Professor Peter Swire[148] and by me elsewhere,[149] the approach of seeking to maintain the secrecy of security flaws as a corporate strategy is widely discredited as ineffective in the computer security literature. Thus, when entities choose to follow the ineffective strategy of security through obscurity, the inevitable consequence of this irresponsible corporate decision becomes an adversarial relationship between the entity and the security researchers who discover and speak publicly about existing problems with the company's vulnerable products. For example, although several reasons exist why vulnerabilities in the smart grid persist,[150] a recent

---

[143] *See id.* at 188–90.

[144] *See CF Disclosure Guidance: Topic No. 2*, U.S. SEC. & EXCHANGE COMMISSION (Oct. 13, 2011), http://sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. And public companies do indeed face the problem of interpreting their disclosure obligations in the event of a breach. For example, recently Wyndham Hotels came under scrutiny in connection with a data breach and an alleged failure to disclose. *See* Elinor Mills, *FTC Sues Wyndham Hotels over Data Breaches*, CNET (June 26, 2012, 9:46 AM), http://news.cnet.com/8301-1009_3-57460551-83/ftc-sues-wyndham-hotels-over-data-breaches/.

[145] Peter J. Toren, *Disclosing Cyber Security Incidents: The SEC Weighs In*, FORBES (June 4, 2012, 1:20 PM), http://www.forbes.com/sites/ciocentral/2012/06/04/disclosing-cyber-security-incidents-the-sec-weighs-in/; *see also* Richard Lardner, *U.S. Pressures Companies to Report Cybercrime*, USA TODAY (June 29, 2012, 6:48 PM), http://www.usatoday.com/money/media/story/2012-06-29/reporting-cybercrime/55921858/1.

[146] Few top law schools have courses in information security law and very few legal academics research in this space. Further, most government agencies have only recently started to consider the impact of information security as part of their duties. Meanwhile, some companies—whether by design or by neglect—sometimes inaccurately describe their privacy and security practices both to the public and to agencies investigating them. *See, e.g.*, *In re* Google Inc., 27 FCC Rcd. 4012 (2012).

[147] Some companies ignore the impact of information vulnerability on society and business partners, externalizing costs and failing to take responsibility for the harms they cause. *See* Jeremy Kirk, *Hacker Group Targets Firms that Hide Security Flaws*, PCWORLD (Mar. 29, 2008, 7:30 AM), http://www.pcworld.com/article/143961/hacker_group_targets_firms_that_hide_security_flaws.html.

[148] Peter P. Swire, *A Theory of Disclosure for Security and Competitive Reasons: Open Source, Proprietary Software, and Government Systems*, 42 HOUS. L. REV. 1333, 1337 (2006).

[149] *See* Matwyshyn, *supra* note 142, at 162–65.

[150] Although advanced metering infrastructures enable more dynamic generation, distribution, and consumption, smart meters, wireless repeaters, and routers must operate in physically unprotected environments and communicate with potentially hostile consumer systems. What is more, expanded bandwidth requirements tempt system designers to rely on nondedicated and often untrusted networks

IEEE article asserted that one such reason is that "many power industry vendors have limited experience dealing with the vulnerability disclosure process. So software vulnerability problems often produce disagreements between vendors and researchers as to the severity of vulnerabilities and appropriate mitigation efforts."[151] Even when an author of vulnerable code initially cooperates with a researcher who finds a vulnerability, tensions sometimes arise because the researcher may believe that the company is failing to adequately prioritize the release of timely patches.[152] Meanwhile, some companies believe that researchers fail to understand the business realities that sometimes dictate a slower patching process.[153]

In other words, complications and legal wrangling frequently arise when software vulnerabilities are first discovered. Because the security researcher who has discovered the vulnerability is usually unaffiliated with the vendor, the researcher is faced with the issue of ascertaining the proper method of disclosing the sensitive vulnerability information, particularly if the author of the vulnerable product is uncooperative.[154] Researchers are

because of their lower costs. A combination of expanded technology dependencies and greater public exposure will increase potential impacts from software vulnerabilities discovered within these systems. Additional difficulties arise for utilities during the deployment of updates or patches because systems are so spread out geographically, network bandwidth is limited, or testing environments and procedures are inadequate. *See What the Power Industry Has to Learn About Cyber Vulnerability Disclosure*, *supra* note 116.

[151] *Id.*

[152] Companies also sometimes attempt to silence their critics by threatening suit against the researchers and academics seeking to stimulate the social conversation around information security. *See, e.g.*, JONES & SIMONS, *supra* note 124. Even legal academics working in the information security space and elite academic presses are not immune from receiving legal correspondence voicing corporate displeasure over academic speech highlighting histories of vulnerability. *See* Letter from Timothy Blank, Dechert LLP, on Behalf of Monster.com, to author (Sept. 24, 2009) (on file with author).

[153] *What the Power Industry Has to Learn About Cyber Vulnerability Disclosure*, *supra* note 116.

[154] Several different methods have been used historically for vulnerability speech. Sometimes information about vulnerabilities has been released through public mailing lists such as Bugtraq or websites. Sometimes "responsible vulnerability disclosure" is used. Responsible vulnerability disclosure generally refers to contacting the author of the vulnerable code and perhaps a computer emergency response team before engaging in public vulnerability speech to give the author a reasonable time frame to fix the problem and create a patch before public disclosure. The goal of responsible disclosure is to minimize the likelihood of an attack exploiting the vulnerability and harming the public by having a patch available at the time the vulnerability becomes publicly known. Many technology vendors maintain formal vulnerability management and disclosure policies, acknowledging their willingness to work with researchers to release fixes in a timely fashion. For example, Microsoft has the Coordinated Vulnerability Disclosure practice to document its handling of occurrences. *See Coordinated Vulnerability Disclosure*, MICROSOFT SECURITY RESPONSE CENTER, http://www.microsoft.com/security/msrc/report/disclosure.aspx (last visited Mar. 21, 2013). Google acknowledges and provides a financial reward to researchers who initially disclose the vulnerability information privately to ensure they can release an appropriate fix before the information is publicly released. *Vulnerability Reward Program*, GOOGLE APPLICATION SECURITY, http://www.google.com/about/company/rewardprogram.html (last visited Mar. 21, 2013).

aware that some companies may seek to criminally prosecute security-vulnerability researchers in connection with vulnerability speech.[155]

Perhaps then we should simply offer aggressive protection to all vulnerability speech and simply carve it out legislatively as protected speech? Unfortunately, while direct, this approach is neither feasible nor desirable. The reality of the information security research "scene" is too nuanced. Although an intellectually vibrant research scene exists in information security, it is characterized by a high degree of fluidity in the demographics and motivations of its participants. The community is also rapidly growing in its size and morphing in its composition.[156] The definition of who is an "information security researcher," what constitutes appropriate credentials and skills,[157] and what is "reasonable" conduct in this space are all malleable constructs; asking different individuals will generate substantially different answers.[158] Even in the most elite or "1337"[159] levels of the information security community, disagreements are increasing over reasonable norms of conduct, and simultaneously, misunderstandings regarding legal limitations on researcher conduct are pervasive. Internal ethical differences in the information security

[155] The recent case of Andrew "Weev" Auernheimer highlights the tension between computer security researchers and companies who are willing to criminally prosecute individuals who disclose security issues in their operations. For a discussion of the Weev case, see, for example, Matt Blaze, *AT&T iPad Hacker's Real Crime Was Embarrassing the Wrong People*, WIRED (Nov. 27, 2012, 6:30 AM), http://www.wired.com/opinion/2012/11/att-ipad-hacker-when-embarassment-becomes-a-crime/.

[156] For example, the size of the DEF CON conference dramatically increases each year, with over 6000 people attending in 2011. *See* Seth Rosenblatt, *Attendance: Touring Black Hat and DefCon 2011*, CNET (Aug. 10, 2011, 4:00 AM), http://news.cnet.com/2300-1009_3-10008941.html.

[157] In fact, some job advertisements for elite security jobs specify that the desired applicants should not be credentialed with the methods that are fast becoming common for new entrants into the information security space, such as Certified Information Systems Security Professional, or CISSP, certification. One prospective employer described the qualifications he is seeking in his future information security employee thusly: "I'm hiring an information security analyst. Must be passionate about security. Must not have CISSP. Must not wear pants." Info Security Jerk, *@infosecjerk*, TWITTER (Aug. 11, 2012, 9:47 PM), https://twitter.com/infosecjerk/status/234511282559127552.

[158] The motivations of researchers in this space vary: a sense of social purpose and altruism motivates some, desire for fame and individual brand building drives others, and sometimes financial gain is the motivating factor. Similarly, excluding corporate speakers from the vulnerability speech ecosystem purely because of their financial motivations would eliminate some of the most important voices from the information security debate. It is this definitional ambiguity that renders any calls for blanket statutory protection for vulnerability speech legislatively unworkable. In the words of well-known information security researcher, Dino Dai Zovi, "ProTip: referring to hackers as a singular group is like referring to Native Americans as a singular group. Most things aren't universal." Dino A. Dai Zovi, *@dinodaizovi*, TWITTER (July 30, 2012, 9:09 AM), https://twitter.com/dinodaizovi/status/229972056203210752. For an argument in favor of statutory protection for security vulnerability disclosure, see, for example, Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1083–86 (2011).

[159] "1337" is the hacker slang spelling of "leet" or elite. It is a term of honor bestowed on only the most skilled members of the hacker community. *See 1337*, URBAN DICTIONARY, http://www.urbandictionary.com/define.php?term=1337 (last visited Mar. 21, 2013).

community are significant, particularly around two issues: first, the issue of "dropping 0-day,"[160] meaning a release of a zero-day exploit without offering the author of vulnerable code the opportunity to cure the deficiencies prior to vulnerability speech; and second, private commercial sales of zero-day exploits, meaning the sale of vulnerability speech about previously unknown vulnerabilities to someone other than the author of the code.[161] Leaving the resolution of these issues solely to the community of technologists involved in vulnerability speech is, therefore, simply not feasible.[162] In part because of these rifts and the growing involvement of the broader (sometimes technology-unsavvy) business community in the code ecosystem, legal challenges and criminal prosecutions in connection with vulnerability speech are fast becoming an inevitability.[163] The recent prosecution and conviction of Andrew "Weev" Auernheimer and the information security community's vociferously negative reaction to the conviction serve as a clear harbinger of legal battles to come with respect to

---

[160] *See, e.g.*, *Dear Bruce—On Zero Days*, ROGER'S INFO. SECURITY BLOG (Jan. 31, 2012, 5:35 AM), http://www.infosecblog.org/2012/01/dear-bruce-on-zero-days/.

[161] Charlie Miller, The Legitimate Vulnerability Market: Inside the Secretive World of 0-Day Exploit Sales 2 (May 6, 2007), http://weis2007.econinfosec.org/papers/29.pdf (describing the emergence of a commercial market for zero-day exploits).

[162] The dominant perception in the community is that the researcher who found the vulnerability—like a person who finds a quarter on a deserted street—gets unrestricted dominion over its fate. Yet, whether this dominion is fettered by certain ethical norms is hotly debated. Not everyone behaves in a manner similar to the reasonable conduct of Barnaby Jack, his employer, and the ATM company. In the words of one security researcher:

> As a computer security researcher, there are many options available after discovering a vulnerability in a high-profile application or operating system. She may choose to report the vulnerability to the vendor, or simply announce it publicly without vendor notification. Such a choice may be made in order to increase her reputation or add to her resume. She may choose to sell the information on the black market, but faces potential criminal prosecution for such an action. Finally, she may choose to attempt to sell this information to a legitimate buyer. Such legal buyers may include government agencies, commercial tool suppliers, large penetration testing and consulting firms, intrusion detection companies, and subscription services.

Id.

[163] Especially as payment for exploits becomes a dominant approach through "bug bounties," "pwn" hacking contests for prize money, and private sales to purchasers (other than the author of the vulnerable code), the schisms in the community are increasingly apparent. For example, two hacking contests at the same conference recently reflected the tension over these different community norms: in one, the contestants were not required to disclose their exploitation techniques, only the details of the crash that led to the vulnerability; while in a second, contestants were obligated to disclose the details of the vulnerability as well as their exploit in order to win. Consider the two hacking contests at the CanSecWest conference in 2012, TippingPoint's Pwn2Own and Google's new Pwnium. As part of Pwn2Own, the contestants did not have to disclose their exploitation techniques or anything other than the details of the crash that led to the vulnerability. In Google's Pwnium contest, by contrast, participants must relinquish the details of the vulnerability as well as the exploit. *See* Dennis Fisher, *PinkiePie Strikes Again, Compromises Google Chrome in Pwnium Contest at Hack in the Box*, THREAT POST (Oct. 10, 2012, 9:48 AM), http://threatpost.com/en_us/blogs/pinkiepie-strikes-again-compromises-google-chrome-pwnium-contest-hack-box-101012.

permissible methods of vulnerability disclosure.[164] Therefore, courts will likely soon need to resolve the First Amendment status of vulnerability speech specifically and informational speech generally. With this impending resolution in mind, the next Part offers one possible approach for these looming cases, an approach that more directly incorporates Redish's notion of "high social value" into an informational speech framework by using the two factors detailed in the preceding section—the presence of positive incidental effects and information scarcity.

III. THE REPURPOSED SPEECH SCALE

In 1919, the Supreme Court famously said, "[T]he character of every act depends upon the circumstances in which it is done. The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic."[165] However, sometimes announcing the existence of a fire in a crowded theater—or identifying a security problem in a nuclear reactor[166]—can result in saving hundreds of lives. The key is context, specifically the nature of the incidental effects of the speech and the reasonableness of its time, place, and manner.

In the case of informational speech such as vulnerability speech, the doctrinal difficulty arises from its possible dual purpose. It is not obvious how to determine when informational speech aims to contribute to the public debate and when it constitutes merely a tool to facilitate criminal

---

[164] Auernheimer was prosecuted and convicted of conspiracy to access a computer without authorization and fraud in connection with personal information. He had discovered a security hole in an AT&T website that leaked customer information and captured leaking data of over 100,000 subscribers using a script. He then allegedly reported the existence of the hole to the press, but failed to contact AT&T prior to disclosure in order to provide an opportunity to patch. Nor did he post the existence of the hole to a mailing list for security vulnerabilities—a commonly used traditional method of disclosing known vulnerabilities. For a discussion of the facts leading up to the prosecution of Auernheimer, see, for example, Kim Zetter, *Hacker Found Guilty of Breaching AT&T Site to Obtain iPad Customer Data*, WIRED (Nov. 20, 2012, 4:52 PM), http://www.wired.com/threatlevel/2012/11/att-hacker-found-guilty/; see also Criminal Complaint, United States v. Auernheimer, No. 11-4022 (CCC) (D.N.J. Jan. 13, 2011), *available at* http://www.wired.com/images_blogs/threatlevel/2011/01/Spitler-Daniel-et-al.-Complaint.pdf. For a discussion of the reaction of the information security community, see, for example, Andrea Peterson, *How Convicting a Troll Threatens the Cybersecurity Community*, THINKPROGRESS (Nov. 27, 2012, 7:30 PM), http://thinkprogress.org/security/2012/11/27/1244461/how-convicting-a-troll-threatens-the-cybersecurity-community/?mobile=nc. AT&T's Chief Security Officer explained to the press that the data capture was enabled by AT&T's decision to prepopulate e-mail addresses to increase customer convenience. *See* Matt Buchanan, *The Little Feature that Led to AT&T's iPad Security Breach*, GIZMODO (June 19, 2010, 9:19 PM), http://gizmodo.com/5559686/. Auernheimer is appealing his conviction. *See, e.g.*, Zetter, *supra.*

[165] Schenck v. United States, 249 U.S. 47, 52 (1919) (citation omitted). Although this portion of *Schenck* was likely effectively overruled by *Brandenburg v. Ohio*, 395 U.S. 444 (1969) (per curiam), the quote remains well known by the public.

[166] *See* Matthew Harwood, *Nuclear Power Plants Vulnerable to Attack, Former CIA Officer Says*, SECURITY MGMT. (Mar. 16, 2010), http://www.securitymanagement.com/news/nuclear-power-plants-vulnerable-attack-former-cia-officer-says-006870.

conduct. By blending the Redish informational speech approach with the stronger focus on context that is visible in the harm-based approaches from the code speech cases and *O'Brien*, this Part offers a new "repurposed speech scale" approach to instructional or informational speech. It is an approach that uses the time, place, and manner of the speaker's communication to determine whether the speaker's dominant communicative intent[167] was salutary or criminal. Thus, the two hallmark features of the repurposed speech scale are its contextual sensitivity and its technology neutrality—a focus on speakers' reasonable conduct *across all media* in mitigating incidental harms arising from their informational speech.

In the context of vulnerability speech, many security researchers perceive themselves to be engaging in scientific and academic commentary, even if they are employed in the private sector. They also may view themselves as participating in breaking important news on topics of public interest. Or, depending on their employment situation, they may see themselves as whistleblowers,[168] alerting the world to unsafe business practices.[169] In the words of one such disclosing researcher who faced suit as a result of his disclosure, "I needed to do what's right for the country and for the national critical infrastructure."[170] However, a legally trained observer—rightly or wrongly—may perceive some security researchers to be acting as vigilantes or merely as participants in a criminal enterprise.[171] And sometimes researchers' conduct may indeed cross the line into illegality. The key is crafting a flexible, technology-neutral standard to guide researchers' conduct.

---

[167] Intent is a logical fulcrum in this case because of the structure of criminal law determinations of responsibility for conduct. For a discussion of criminal intent, see, for example, John F. Decker, *The Mental State Requirement for Accomplice Liability in American Criminal Law*, 60 S.C. L. REV. 237, 245–60 (2008).

[168] For example, it is likely that when Michael Lynn disclosed the existence of a vulnerability in Cisco routers—a disclosure that resulted in an FBI probe and suit—he viewed himself to be acting as a whistleblower. *See, e.g.*, Kim Zetter, *Whistle-Blower Faces FBI Probe*, WIRED (July 29, 2005), http://www.wired.com/politics/security/news/2005/07/68356?currentPage=all.

[169] For a discussion of the different role of identities of individuals engaging in technology-assisted disclosure and how it might inform an analysis of the disclosure under the First Amendment, see, for example, Bellia, *supra* note 133. However, what researchers sometimes forget is that whistleblowers frequently face criminal sanctions, despite the social value of their speech. For example, in the Pentagon Papers case, a criminal prosecution against Daniel Ellsberg continued even though the case against the New York Times was dismissed. *See* DANIEL ELLSBERG, SECRETS: A MEMOIR OF VIETNAM AND THE PENTAGON PAPERS 444 (2002); *see also* N.Y. Times Co. v. United States, 403 U.S. 713 (1971).

[170] See Bruce Schneier, *Cisco Harasses Security Researcher*, SCHNEIER ON SECURITY (July 29, 2005, 4:35 AM), http://www.schneier.com/blog/archives/2005/07/cisco_harasses.html.

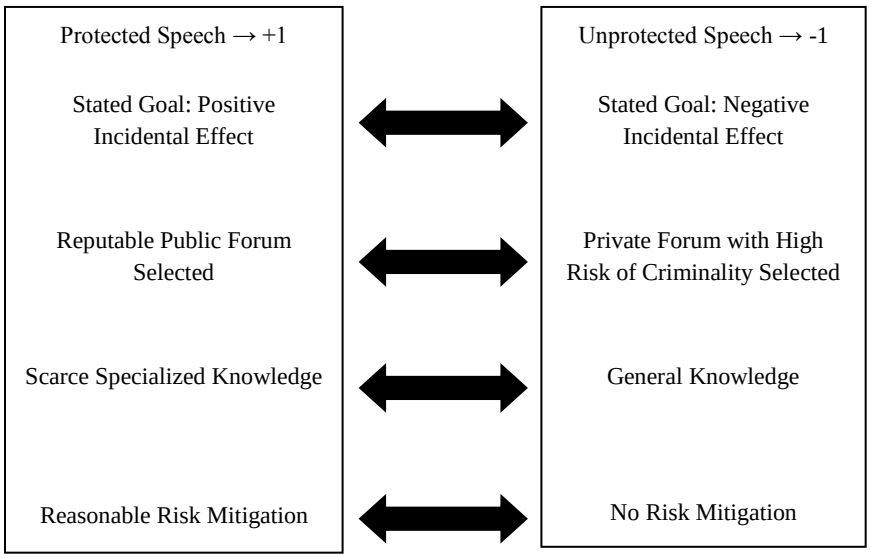
[171] *See* discussion of the Aurnheimer case, *supra* note 164.

A. Combining Code Speech with Informational Speech: The Repurposed Speech Scale

As I have argued above, the *O'Brien* approach,[172] which courts have sometimes applied to code, is actually a good conceptual fit for building a First Amendment framework for analyzing informational speech and its negative incidental effects.[173] A framework derived from *O'Brien* presents courts with flexibility to weigh individualized circumstances in cases before them, while simultaneously preserving general rubrics of relevant information as part of a broader framework across cases.

As Figure 1 demonstrates, four factors can be used to create a repurposed speech scale in order to determine whether a particular type of informational or instructional speech warrants First Amendment protection, regardless of its potential repurposing for criminality.

FIGURE 1: THE REPURPOSED SPEECH SCALE FOR INFORMATIONAL SPEECH



[172] *See supra* text accompanying notes 94–97.

[173] A test reliant on determining the functionality of the speech itself rather than its incidental effects would be a fruitless exercise. In a similar vein, Professor John Hart Ely has argued:

> [B]urning a draft card to express opposition to the draft is an undifferentiated whole, 100% action and 100% expression. It involves no conduct that is not at the same time communication, and no communication that does not result from conduct. Attempts to determine which element "predominates" will therefore inevitably degenerate into question-begging judgments about whether the activity should be protected.

John Hart Ely, *Flag Desecration: A Case Study in the Roles of Categorization and Balancing in First Amendment Analysis*, 88 HARV. L. REV. 1482, 1495 (1975).

As Figure 2 demonstrates, this more general repurposed speech scale can then be customized to assess the case study of vulnerability speech.[174] Specifically, the four factors of the repurposed speech scale are as follows: (1) whether the stated goal of the speaker identifies an interest in generating positive incidental effects from the speech or negative incidental effects from the speech, regardless of the content of the speech; (2) whether the speaker selects a reputable forum in the public eye for his speech, in lieu of a private forum where criminality is the more likely result; (3) whether the speech represents scarce specialized knowledge possessed by only a few experts or whether the speech reflects easily available general knowledge; and (4) whether the speaker has engaged in reasonable risk mitigation steps in order to limit the potential negative incidental effects of his speech. The presence of each of these factors means a high score, the absence a low score. These four factors should be analyzed concurrently and tallied together in order to create an overall assessment of the speaker's objective communicative intent—either one more in line with furthering debate[175] or one more in line with furthering criminality.[176] A high score on the scale indicates the appropriateness of First Amendment protection for the speech. A low score signals a likelihood of criminal intent and inappropriateness of First Amendment protection. A score in the middle should be construed in favor of First Amendment protection for the informational speech, erring on the side of overprotection to avoid chilling future speech.

---

[174] Professor David McGowan has correctly argued that to the extent code facilitates unlawful behavior, it should be covered under incitement, which requires that the state demonstrate a likelihood that an act will cause harm in order to justify its regulation. *See* McGowan, *supra* note 43, at 1576–78. Lee Tien similarly explains that:

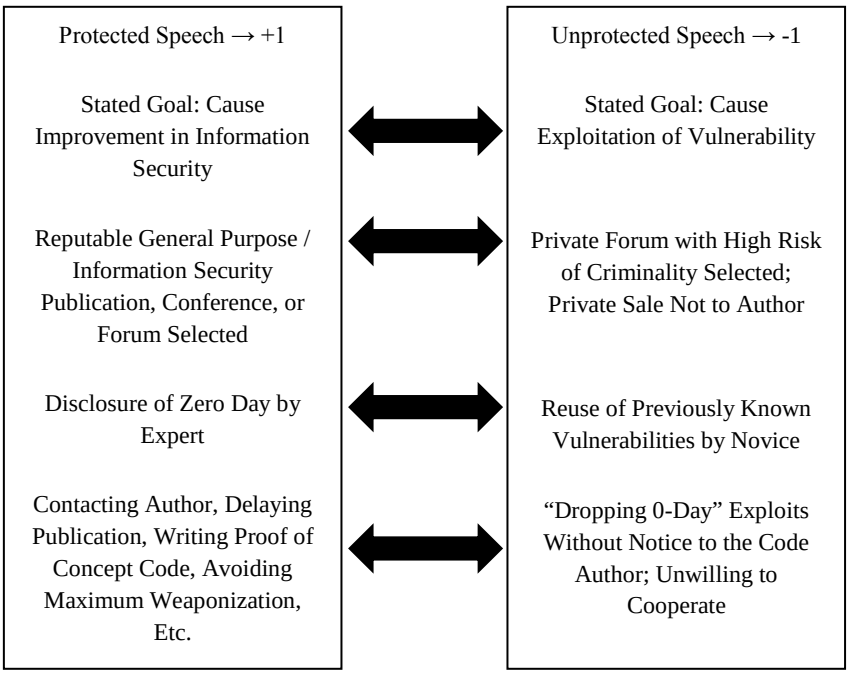
> There's no doubt that the actor is speaking, but he might "also" or "really" be doing something else. . . . Crucially, Alice's act of publishing her software in itself causes no harm. The fear is that others may use her software to cause harm. The risk of harm is difficult to distinguish from that associated with the publication of many kinds of information.
>
> In short, there's nothing special about software for purposes of First Amendment coverage. The First Amendment need not be "extended" for software to be covered as "speech."

Tien, *supra* note 41, at 635–36.

[175] This concern was highlighted by the Second Circuit in *Commodities Future Trading Commission v. Vartuli*, 228 F.3d 94, 109–12 (2d Cir. 2000).

[176] As Lee Tien explains, "Even if the virus author merely posts the source code and fails to release it in active form, the issue remains whether the posting was done with an intent to communicate. . . . There is no question that people study viruses and other dangerous software in order to prevent or relieve harm. . . . When such publications aim to alert the world to these dangers, their intent is clearly communicative." Tien, *supra* note 41, at 675–76.

FIGURE 2: THE REPURPOSED SPEECH SCALE FOR INFORMATIONAL SPEECH: APPLICATION TO VULNERABILITY SPEECH



1. The Speaker's Goal and the Incidental Effects of the Informational Speech.—The first factor asks whether the speaker's self-identified communicative goal relates to positive incidental effects expected to arise from the speech. In other words, it includes a subjective intent assessment from the perspective of the speaker. In this manner, the scale is informed by case law that defines incitement in terms of both the speaker's intent and the act's likely effect, but not the content of the speech itself. This first factor incorporates the spirit of Redish's first and second informational speech factors through asking the speaker for his perception of the likely positive or negative incidental effects of his speech.[177] Further, this factor picks up on the notion of intent articulated in *O'Brien*, that "the person engaging in the conduct intends thereby to express an idea,"[178] and it seeks to ascertain what that idea was from the subjective perspective of the speaker. Returning to *Rice v. Paladin*[179] and the criminal intent stipulation therein, this factor differentiates cases where

[177] *See* Redish, *supra* note 7, at 90.

[178] United States v. O'Brien, 391 U.S. 367, 376 (1968).

[179] Rice v. Paladin Enters., Inc., 128 F.3d 233 (4th Cir. 1997).

speakers directly express interest in furthering criminality from those cases where criminality is merely an unfortunate byproduct of a well-intentioned, socially concerned speaker. In other words, this factor differentiates single-purpose informational speech, which primarily facilitates criminality, from dual-purpose informational speech, which might incidentally further criminality but the primary purpose of which is to push forward debate on matters of public concern.

Applying this first factor of the repurposed speech scale approach—whether the stated goal of the speaker is generating positive incidental effects with his speech—to the case study of vulnerability speech, courts would look to the asserted rationale behind an information security researcher's vulnerability disclosure. Subjectively, from the perspective of the information security researcher, the court would ask whether the goal of the disclosure was to improve the state of information security in society and to protect consumers or national security from harm. Therefore, an assertion of a deep concern over mitigating information vulnerability and improving the integrity of code would afford this speech a high score on this factor in the scale. However, a stipulation by the researcher that the purpose of a particular disclosure is to facilitate the criminal exploitation of vulnerabilities would afford this speech a low score on this factor in the scale.[180]

2. The Reputation of the Speaker's Selected Forum.—The second element incorporated into the repurposed speech scale relates to the particular forum the speaker selects for his speech. If the speaker selects a highly reputable forum in the public eye—a forum where his speech is likely to stimulate social debate—this forum selection would earn the speech a high score on this second factor of the scale. However, if the speaker selects a private forum for his speech, particularly a private forum known for a high risk of criminality, this removal of his speech from the public space for debate would warrant a low score for this factor. This factor reflects a transformation of Redish's first and second factors, refocusing them more on the context of the speech and the known audience

[180] In other words, courts would not look to objective indicators of intent but rather to the speaker's subjective asserted rationale for the disclosure as previously asserted to the media, in the record or through testimony at the time of trial. This factor gives the benefit of the doubt to the speaker by design. For example, the motivations of many information security researchers looking into election systems have been articulated by Professor Edward Felten: "We have created and analyzed the code in the spirit of helping to guide public officials so that they can make wise decisions about how to secure elections." Teresa Riordan, *Researchers Reveal 'Extremely Serious' Vulnerabilities in E-Voting Machines*, NEWS AT PRINCETON (Sept. 13, 2006, 12:46 PM), http://www.princeton.edu/main/news/archive/S15/81/65O23/index.xml?section=topstories. Corporate researchers who conduct research on election software frequently volunteer their time to do so. They are frequently driven by a sense of concern for preserving the integrity of the electoral process and the future of our electoral system.

present in that context.[181] Taking speech out of the public eye limits the possibility for stimulating debate; in the opinion of at least some courts, the public eye renders speech less threatening and less dangerous.[182]

In the context of vulnerability speech, applying the second factor of the scale, whether the speaker selected a reputable forum in the public eye or a private forum with a high risk of criminality, means that an information security researcher who chooses to engage in a vulnerability disclosure in a respected information security publication or chooses to present his research at a major information security conference is selecting a reputable forum. His choice of forum offers wide exposure for his research in a manner likely to stimulate debate both inside the information security community and in the public at large. In other words, he creates a situation where debate and counterspeech can occur. Therefore, the choice of a forum in the public eye means the communication deserves a high score on this factor of the scale. If, however, a researcher selects to limit access to his speech by sharing only in a private forum or in a forum where the audience is predominantly composed of reputed cybercriminals, this researcher chooses to target a different kind of audience for his speech—one more likely to be interested in using his research for criminality rather than the furtherance of public debate. Similarly, if a researcher chooses to sell his exploits in private sales,[183] the researcher is choosing to remove his speech from the public debate rather than to contribute it to society. Consequently, this communication in a private forum would mean a low score for the speech on this factor in the scale. Why is this the case? In the words of Professor Dan Burk, the debate over code and speech invokes

---

[181] *See* Redish, *supra* note 7, at 90. This prong also incorporates insights from Volokh's first prong. Professor Kent Greenawalt has also highlighted the distinction between public and private communications, explaining that "justifications for free speech . . . do not reach communications that are simply means to get a crime successfully committed." KENT GREENAWALT, SPEECH, CRIME, AND THE USES OF LANGUAGE 85 (1989). Greenawalt asserts that public advocacy, meaning advocacy that refers to a "right, overall welfare, or some historical, philosophical, political, or religious view," has substantial value as expression as it reflects an effort to persuade the public of the wisdom of a particular course of action or view rather than an attempt to convince a person or a group of persons to commit a crime. *Id.* at 261.

[182] *See, e.g.*, United States v. Carmichael, 326 F. Supp. 2d 1267, 1288 (M.D. Ala. 2004) (holding that drug defendants with a website of "wanted" agents were not enough of an "imminent" threat for a protective order because there was no evidence that the communication "authorized, ratified, or directly threatened acts of violence," and the public nature of the communication supported this conclusion (quoting NAACP v. Claiborne Hardware Co., 458 U.S. 886, 929 (1982))); Sheehan v. Gregoire, 272 F. Supp. 2d 1135, 1143 (W.D. Wash. 2003) (holding that when the operator of a website critical of law enforcement challenged a statute regarding publishing personal information of officers, release of the information, without more, does not constitute a true threat). As Justice Brandeis explained, "If there be time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech . . . ." Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring).

[183] I refer here to situations other than receiving a bug bounty from the author of the vulnerable code.

"the venerable literary debate as to whether text constitutes *Logos*—a thing said, or *Poiema*—a thing made."[184] As vulnerability speech becomes private and commodified in sale, it starts to resemble a "thing made" more than speech, and consequently it renders itself more regulable as a potentially dangerous product less worthy of First Amendment protection.[185]

For example, in 2012, a teen using the handle Pinkie Pie won the Google Pwnium contest[186] and triumphantly caused the Chrome browser to redirect to a website emblazoned with his symbol—a pink My Little Pony image.[187] Google awarded Pinkie Pie $60,000 in prize money, Pinkie Pie explained his exploit, and Google thanked him for his good work, which it applied to correct its browser's security issue.[188] Meanwhile, at the same conference where Pinky Pie's My Little Pony proudly trumpeted his achievement in Pwnium, a team from the security firm Vupen discovered a flaw in another Google product.[189] However, unlike Pinky Pie, who was glad to contribute to improving the product, and thus information security in general, Vupen's motivations appeared to involve no interest in improving the product's security or contributing to the public debate over information security in the United States: according to the chief executive of this company, the company "wouldn't share this with Google for even $1 million."[190] He continued, "We don't want to give them any knowledge that can help them in fixing this exploit or other similar exploits. We want to keep this for our customers."[191] Applying the chosen forum factor to these two instances of vulnerability speech, while Pinkie Pie's speech demonstrates an interest in sharing the information in a reputable public

---

[184] Burk, *supra* note 41, at 120.

[185] Contract law doctrines with respect to permissible subject matter and public policy would support setting aside contracts for sales of vulnerabilities as potentially unenforceable. Further, sales of attacks that exploit vulnerabilities are likely regulable on grounds of interstate commerce and national defense.

[186] *See* Kim Zetter, *Teen Exploits Three Zero-Day Vulns for $60K Win in Google Chrome Hack Contest*, WIRED THREAT LEVEL (Mar. 9, 2012, 7:37 PM), http://www.wired.com/threatlevel/2012/03/zero-days-for-chrome/.

[187] *Id.*

[188] *Id.*

[189] *See Vupen Strikes Again: French Team Cracks IE 9 in Pwn2Own Hack Contest*, INFO SECURITY (Mar. 9, 2012), http://www.infosecurity-magazine.com/view/24441/vupen-strikes-again-french-team-cracks-ie-9-in-pwn2own-hack-contest/.

[190] Andy Greenberg, *The Zero-Day Salesmen*, FORBES, Apr. 9, 2012, at 40, 42. In a rather public Twitter spat with Google, Vupen released a video showing that it could penetrate a machine running Chrome but provided no information to Google that facilitated correcting the vulnerability. Google responded by identifying a possible source of the problem. Vupen then accused Google of downplaying its vulnerabilities and called it "pathetic." *Id.* at 44. As might be expected, this Twitter barb triggered a retort from Google security staffers who condemned Vupen for disregarding users' privacy and called Vupen's CEO an "ethically challenged opportunist." *Id.*

[191] *Id.* at 42. Analysts have asserted that Vupen's clients pay around $100,000 annually for a subscription plan, "which gives them the privilege of shopping for Vupen's techniques." *Id.*

forum to improve a vulnerable product, Vupen's vulnerability speech takes the information out of the public eye and would score lower on this factor in the repurposed speech scale.

3. The Scarcity of the Speaker's Contributed Knowledge.—The third factor in the repurposed speech scale relates to the scarcity or pervasiveness of the knowledge contributed by the speech. As Part II explained, although perhaps it is counterintuitive, information that is known only by a small, specialized group of experts, if shared, may be most likely to contribute novel arguments to the public debate.[192] Consequently, the willingness of experts to contribute their skills for the purposes of furthering a social policy debate constitutes a high-value type of speech[193] deserving a high score on this factor in the scale, even in instances where the speech can be repurposed to facilitate criminal activity. However, in line with the court's analysis in *Rice v. Paladin*, if the knowledge contributed by the speech is already easily accessible to members of the public and it simultaneously heightens the possibility of criminality, this type of general knowledge speech is more appropriately scored with a low value on this factor in the scale. It is unlikely to contribute meaningfully to the public debate. This third factor is an inversion of Redish's third factor relating to information availability: while Redish asserted that information already publicly available should trigger a higher level of protection,[194] I would assert the contrary. Because of the potential high social value and its simultaneous scarcity, commentary by experts with specialized knowledge may warrant higher levels of protection in the context of informational speech than, for example, a mere aggregation of readily available Internet information reflecting only the "sweat of the brow" of a novice. In this way, it might be argued that Redish's fourth factor, the potential value to the public of the revealed information, is implicitly incorporated within this third factor of the repurposed speech scale.

In the context of vulnerability speech, this third factor—whether the knowledge constitutes scarce, specialized knowledge or generally available knowledge—would translate into affording the public disclosure of zero-day exploits by information security experts a high score on this factor in the scale. For example, the ability of an information security researcher to examine a voting machine and, in only a few hours, compromise the integrity of a mock election is a skill held by a relatively small number of researchers. Yet, having this informational speech contributed to the public debate over the desirability of electronic voting machines is of paramount

[192] Courts frequently look to experts to guide the determination of disputes in cases. Here, it can be argued that society benefits through encouraging experts to contribute their esoteric knowledge pro bono to the public conversation around issues of social importance. Thus, a thumb on the judicial scale in favor of expertise and specialized knowledge is not a radical suggestion.

[193] Information value is driven by scarcity. *See supra* notes 135–39.

[194] *See* Redish, *supra* note 7, at 90–91.

importance. Meanwhile, the mere aggregation or republication of known vulnerabilities and exploit code would receive a low score for this factor: the risks outweigh the novelty of the contribution to the social conversation.

4. The Speaker's Reasonable Risk Mitigation of Negative Incidental Effects.—Finally the fourth factor in the scale, the extent of reasonable risk mitigation[195] by the speaker, asks whether the speaker considered and actively sought to minimize likely negative incidental effects[196] that would result from his speech. In circumstances where evidence exists that the speaker used reasonable care to mitigate against the possible harms arising from the time, place, and manner of his speech,[197] these reasonable efforts would mean a high score on this factor in the scale. If, however, the speaker chose to ignore available reasonable measures for mitigating the possible damaging impacts of his speech and proceeded to speak in a manner demonstrating disregard of any likely harm, this lack of care would mean a low score on this factor.[198] Thus, this factor is an offshoot of Redish's first and second factors relating to the likelihood and severity of potential criminality that may result, but reframes them using the language of *O'Brien*.[199]

In the context of vulnerability speech, the fourth factor relating to reasonable risk mitigation would be operationalized by analyzing whether the researcher limited damage likely to be caused because of his vulnerability disclosure and exploit. In other words, to what extent was the researcher willing to take affirmative steps to minimize the likelihood that criminal exploitation of the discovered vulnerability will occur? Because the researcher sits in the optimal position to analyze the avenues of possible harm resulting from his vulnerability speech, the researcher is in the best

---

[195] In response to this type of argument, prior scholarship has also argued that unlike other code, compiled malicious programs raise different issues because they are functioning. *See* Tien, *supra* note 41, at 669–70. As such, a compiled exploit arguably may be more closely akin to a weapon such as a bomb than to a book or a pamphlet, with the sole purpose of causing harm. Some authors argue that:

> [P]osting code is like leaving a loaded gun out on a windowsill: if someone picks up the gun and shoots a puppy, the liability of the gun owner is not assessed under incitement law. This is true even if the gun owner left the gun for communicative purposes—to show off the stock, or protest antigun laws.

John Greenman, *On Communication*, 106 MICH. L. REV. 1337, 1375 (2008).

[196] In other words, the assessment is an analysis of harm minimization.

[197] This analysis is not an analysis of the content of the speech, merely its negative and positive incidental effects.

[198] For example, in the *Hustler* case, the publisher included meaningful cautionary language as part of an article discussing high-risk activities to mitigate the risk of a reader attempting the activities described. Herceg v. Hustler Magazine, Inc., 814 F.2d 1017, 1018 (5th Cir. 1987).

[199] Although temporal proximity between an initial communication and harm has traditionally been considered in incitement analysis, today's reality of mixed media in communications complicates a linear temporal analysis. This is because services such as YouTube arguably preserve at least a portion of the potency of a live interaction long after its occurrence in physical space.

position to engage in the first round of mitigation against these harms. For example, courts might look to whether the researcher was willing to cooperate with the author of the vulnerable code in order to correct the vulnerability both before and after his vulnerability speech. A court might also ask whether the researcher wrote proof of concept code in a manner to intentionally minimize the possible extent of exploitability or weaponization of the vulnerability in the course of proving its existence.[200] If, however, the researcher seemed to be simply interested in the reputational glory of "dropping 0-day"[201] and was unwilling to reasonably cooperate with or notify the author of the code prior to releasing exploit code into the wild, these actions would push the speech toward a low score on this factor in the scale.

For example, in 2009, researchers from the security firm IOActive found a series of vulnerabilities inside smart grid technologies. Although they identified the vulnerable technologies in question, because their goal was to stimulate conversation inside the security research community and to catalyze SCADA[202] security improvements,[203] they did not disclose the identities of the particular companies whose products contained the vulnerabilities: they were cautious to limit the risk of active exploitation of the vulnerabilities.[204] However, as later vulnerability disclosure in the SCADA space demonstrates, this approach is not always the norm, and tensions have arisen inside the information security community that will inevitably end in the courts. For example, a different team of researchers from a different security firm, citing frustrations with smart grid vendors' lack of effort to improve security, handled smart grid vulnerability disclosure in a substantially different manner: not only did the team reportedly publicly identify the numerous vulnerabilities and vendors in question,[205] but they also apparently developed and made available the

---

[200] *See, e.g.*, *Microsoft Security Advisory (921923): Proof of Concept Code Published Affecting the Remote Access Connection Manager Service*, MICROSOFT SECURITY TECHCENTER (June 23, 2006), https://technet.microsoft.com/en-us/security/advisory/921923?.

[201] *See, e.g.*, *id.*

[202] *See* OFFICE OF THE MANAGER, NAT'L COMMC'NS SYS., TECHNICAL INFORMATION BULLETIN 04-1: SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS (2004), *available at* http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf.

[203] In particular, the researchers had focused on the Advanced Metering Infrastructure (AMI), devices that monitor and control the use of energy in homes and businesses. Approximately 2 million of the devices had been deployed at the time of the discovery, and an estimated 17 million devices had allegedly been ordered by utilities. Robert Lemos, *Smart-Grid Firms Need Security Education*, SECURITYFOCUS (Mar. 24, 2009), http://www.securityfocus.com/brief/932.

[204] *See id.*; *see also* Interview with Robert Zigweid, Principle Compliance Consultant for IOActive, in Las Vegas, Nev. (July 27, 2012) (notes on file with author).

[205] According to press reports, the vulnerabilities were found in widely used programmable logic controllers made by General Electric, Rockwell Automation, Schneider Modicon, Koyo Electronics, and Schweitzer Engineering Laboratories. *See* Kim Zetter, *Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software*, WIRED THREAT LEVEL (Jan. 19, 2012, 7:23

exploit code[206] required to take advantage of the vulnerabilities without giving the vendors who authored the code or Department of Homeland Security (DHS) ICS-CERT[207] a chance to intervene and patch it.[208] The researchers asserted that they "didn't want a vendor to jump out in front of the announcement with a PR campaign to convince customers that it wasn't an issue they should be concerned with."[209] Taking this researcher's commentary at face value, the team chose to release the exploit code in lieu of first allowing a public conversation to happen about the vulnerabilities: the team appears to have anticipated that if the products were actively compromised by malicious attackers, the conversation would be short circuited. From the perspective of some officials in the DHS, by releasing exploits before vendors and customers could mitigate the vulnerabilities, these researchers unnecessarily exposed the systems to attack by low-level hackers.[210] While the IOActive vulnerability speech clearly demonstrates an

---

PM), http://www.wired.com/threatlevel/2012/01/scada-exploits/; *see also* Andy Bochman, *Attention Electric Sector: Wired Reports SCADA Exploits in the Wild*, SMARTGRIDNEWS.COM (Jan. 24, 2012), http://www.smartgridnews.com/artman/publish/Technologies_Security/Attention-electric-sector-Wired-reports-SCADA-exploits-in-the-wild-4404.html#.UHB7XNWs16Y. These controllers are used in industrial control systems "to control functions in critical infrastructure such as water, power and chemical plants; gas pipelines and nuclear facilities; as well as in manufacturing facilities such as food processing plants and automobile and aircraft assembly lines." Zetter, *supra*.

[206] The researchers released exploit modules using a tool called Metasploit. Metasploit is a tool used by computer security professionals to test if their networks contain specific vulnerabilities, but it is also an exploit tool used by malicious hackers to find and gain access to vulnerable systems. The vulnerabilities included backdoors, lack of authentication and encryption, and weak password storage that would allow attackers to gain access to the systems. "The security weaknesses also ma[d]e it possible to send malicious commands to the devices in order to crash or halt them, and to interfere with specific critical processes controlled by them, such as the opening and closing of valves." *Id.*; *see also About Metasploit*, METASPLOIT, http://www.metasploit.com/about/ (last visited Mar. 21, 2013).

[207] ICS-CERT is the Industrial Control Systems Cyber Emergency Response Team housed in the Department of Homeland Security. *See The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)*, ICS-CERT, http://www.us-cert.gov/control_systems/ics-cert/ (last visited Mar. 21, 2012). It explains its role as a team that

> coordinates control systems-related security incidents and information sharing with Federal, State, and local agencies and organizations, the intelligence community, and private sector constituents, including vendors, owners and operators, and international and private sector CERTs. The focus on control systems cybersecurity provides a direct path for coordination of activities among all members of the critical infrastructure stakeholder community.

More Information About the Industrial Control Systems Cyber Emergency Response Team, ICS-CERT, http://ics-cert.us-cert.gov/ics-cert/more_information.html (last visited Mar. 21, 2013).

[208] *See* Bochman, *supra* note 205. According to one of the lead researchers on the team, "a large percentage of the vulnerabilities the researchers found were basic vulnerabilities that were already known to the vendors, and that the vendors had simply 'chosen to live with' them rather than do anything to fix them." *Id.*

[209] Zetter, *supra* note 205. Wightman and Peterson, two of the researchers who uncovered the vulnerabilities, allegedly said they wanted to avoid companies issuing statements to customers downplaying the vulnerabilities. *Id.*

[210] "'We have so many of these little scriptkiddies that are looking at these things and that are associating themselves with these anarchist groups,' said the official, who talked to Wired on condition

attempt to mitigate harm and would receive a high score on this mitigation factor of the scale, the second company's vulnerability speech does not show signs of reasonable mitigation on its face and would likely warrant a low score on this factor.[211]

B. The Two Implementations

Two possible vulnerability speech First Amendment scenarios are likely to arise where courts may reach for an instructional or informational speech approach such as the repurposed speech scale described above. The first situation likely to arise relates to a First Amendment challenge to an act of Congress which meaningfully limits the ability of speakers to engage in instructional or informational speech on topics that implicate national security concerns. The second scenario involves criminal prosecutions in connection with instructional or informational speech.

1. Congressional Action Prohibiting Vulnerability Speech.—In the age of Stuxnet[212] and the progressive weaponization of vulnerabilities for national security and offensive use, Congress is demonstrating interest in new "cybersecurity" legislation.[213] In particular, it is likely that private sales of exploits to parties other than the author of vulnerable code will be legislatively prohibited for national security reasons—a prohibition that could potentially overreach and limit security vulnerability research generally. The legal questions around regulating the sales of exploits reflect the underlying tension presciently identified by Professor Dan Farber over a decade ago regarding the erosion of the boundary between commerce and speech.[214]

---

that his name not be used since he was not authorized to speak to the press. 'They want to create problems, and they're just trying to figure out how. And that's very concerning.'" *Id.*

[211] Other security researchers also raise concerns about this idea of "teaching a lesson" to authors of vulnerable code by releasing exploits, noting that this approach is controversial. In the words of one researcher, "I would never think about releasing this stuff." *Id.*

[212] *See, e.g.*, Nate Anderson, *Confirmed: US and Israel Created Stuxnet, Lost Control of It*, ARS TECHNICA (June 1, 2012, 5:00 AM), http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/.

[213] For example, Congress has already placed restrictions on hyperlinking. *See* H. Brian Holland, *Inherently Dangerous: The Potential for an Internet-Specific Standard Restricting Speech that Performs a Teaching Function*, 39 U.S.F. L. REV. 353, 356–66 (2005); *see also* 18 U.S.C. § 842(p) (2006) (criminalizing the distribution, including through the Internet, of bomb-making instructions). As such, hyperlinking to a website is prohibited to the extent that it constitutes a distribution of information that pertains to the manufacture or use of an explosive device with knowledge that the information receiver will use that information to violate federal law. *See, e.g.*, Holland, *supra*, at 367. In one case, an eighteen-year-old was prosecuted under the Antiterrorism and Effective Death Penalty Act for posting mirrored informational materials from other websites, which included instructional information about defeating police tactics and bomb making. *See id.* at 366–72. The prosecution resulted in a plea bargain and a sentence of one year in prison. *See id.* at 370–71.

[214] *See* Farber, *supra* note 57.

According to press accounts, a vibrant gray market has emerged in zero-day exploits. A single zero-day exploit sometimes now sells for as much as $200,000.[215] Although some researchers have long sold exploits, a marked shift appears to have happened just in the last year in the dynamics of the information security community with respect to the prevalence of exploits for sale.[216] Purchasers' uses of the exploits vary and are not traced: some purchasers are governments who use the exploits for spying purposes, while other purchasers may be companies who use the exploits for marketing. Still other purchasers in this vulnerability marketplace are companies who provide a subscription security service to clients,[217] defense contractors,[218] and companies and individuals who act as intermediaries for private buyers.[219] While some security commentators argue in favor of banning exploit sales entirely,[220] intermediaries argue that the prohibition would be fruitless and simply militarily disadvantage the United States in the international marketplace.[221] Many members of the information security community appear to view this as merely an "ethical" difference: they fail to acknowledge the potentially serious legal and national security implications that may accompany U.S. researchers selling zero-day exploits

---

[215] *See, e.g.*, Greenberg, *supra* note 190, at 44. As explained by one security researcher who advocates selling exploits, "There is strong evidence that . . . researchers are now motivated more by monetary gain than prestige." Miller, *supra* note 161. Miller continues,

> There has long been a black market for computer exploits. For a long time, hackers were content to trade or sell exploits amongst themselves, mostly for prestige. Computer security researchers normally followed "responsible" disclosure which entails contacting the vendor and usually receiving acknowledgment when the vulnerability was announced along with the supplied patch. In the last few years, the market for 0-day exploits, those for which there is no available patch, has begun to migrate into the commercial space.

Id.

[216] According to at least one participant, the exploit gray market has "exploded" in the last year: in the words of this intermediary, there are now "more buyers, deeper pockets," the time for a purchase has accelerated from months to weeks, and sellers frequently have twelve to fourteen zero-day exploits every month compared to just four to six a few years ago. *See* Andy Greenberg, *Shopping For Zero-Days: A Price List for Hackers' Secret Software Exploits*, FORBES (Mar. 23, 2012, 9:43 AM), http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/. One single browser exploit sold for $125,000. *Id.*

[217] Firms include TippingPoint, Snosoft, and iDefense. Additional players in the exploit sale industry include smaller firms like Vupen, Endgame, and Netragard. *Id.*

[218] Northrop Grumman and Raytheon are examples. *Id.*

[219] These intermediaries are not always U.S. citizens or interested in preserving the national security of the United States. *See id.*

[220] In the words of one security researcher, Chris Soghoian, industry self-regulation is needed: "Security researchers should not be selling zero-days to middle man firms . . . These firms are cowboys and if we do nothing to stop them, they will drag the entire security industry into a world of pain." *Id.*

[221] On the other hand, intermediaries argue, sales of vulnerabilities are inevitable—just like sales of guns: by failing to participate and outlawing the practice, the United States would only disadvantage itself and its companies. *See id.*

to foreign governments.[222] However, even prominent proponents of vulnerability markets are becoming concerned: in the words of one such researcher, "The fact that the market for vulnerability information favors selling to governments is terrible and needs to be addressed."[223] Exploit sales to foreign countries may quickly become the treason of the 21st century. In the words of one exploit intermediary, "Realistically, we're selling cyberweaponry."[224]

Yet, in the name of protecting national security, particularly with respect to these problematic vulnerability markets, "cybersecurity" legislation may be drafted with overly aggressive language. In such a case, the new legislation might be construed to limit the ability of vulnerability researchers to engage in vulnerability speech in forums in the public eye or even to approach companies with knowledge of vulnerabilities, hoping to assist them in information security improvements to products. While a narrowly crafted legislative prohibition on vulnerability sales to foreign governments that threaten U.S. national security interests would likely survive First Amendment scrutiny, overly broad legislative crafting should not be allowed to limit vulnerability speech protectable under the repurposed speech scale.

2. Criminal Prosecutions.—As the previous sections have explained, fundamental social interests are at stake in improving information security in our democratic process and economy. As the monetary stakes in the business of information security and public awareness of security breaches increase, litigation over vulnerability speech becomes progressively more likely. Further, as the participants in the information security ecosystem increase in number, it also becomes more likely that disclosed exploits will be used by criminals, potentially leading to a criminal prosecution of the researchers who discovered the vulnerabilities for aiding and abetting[225] or

---

[222] *See, e.g.*, Kim Zetter, *Researchers Seek Help Cracking Gauss Mystery Payload*, WIRED THREAT LEVEL (Aug. 14, 2012, 9:00 AM), http://www.wired.com/threatlevel/2012/08/gauss-mystery-payload/.

[223] Charlie Miller, *@0xcharlie*, TWITTER (Aug. 14, 2012, 8:47 AM), https://twitter.com/0xcharlie/status/235402152716152834.

[224] See the comments of Netragard's founder, Adriel Desautels, in Greenberg, *supra* note 216. However, these "cyberwar" scenarios are not the only information security dynamics that may trigger a need for an informational speech analysis. Another such possible scenario might involve people who post instructions or useful information in forums frequented by members of "hacktivist" collectives such as Anonymous.

[225] According to the Model Penal Code, an accomplice has "the purpose of promoting or facilitating the commission of the offense." MODEL PENAL CODE § 2.06(3)(a) (1985). The aider must have the purpose of abetting a specifically identifiable crime and an underlying offense must occur in order to hold the aider criminally responsible.For discussions of aiding and abetting in various contexts, see, for example, Andrei Mamolea, *The Future of Corporate Aiding and Abetting Liability Under the Alien Tort Statute: A Roadmap*, 51 SANTA CLARA L. REV. 79, 109–11 (2011); Eugene J. Schiltz, *Civil Liability for Aiding and Abetting: Should Lawyers Be "Privileged" to Assist Their Clients' Wrongdoing?*, 29 PACE L. REV. 75 (2008); and Angela Walker, Note, *The Hidden Flaw in* Kiobel*:*

conspiring[226] in the criminal act. Other possible criminal charges arising out of vulnerability speech could implicate economic espionage,[227] identity theft or fraud,[228] and even treason,[229] depending on the circumstances.[230] For example, a finder of security vulnerabilities may engage in vulnerability speech in a manner that angers or embarrasses a company with a vulnerable system or product, leading to the prosecution of that individual.[231] Alternatively, the heightened social concern over "cyberwar" and information security may also lead to an increase in criminal prosecutions for aiding and abetting[232] or conspiring to commit computer intrusion in connection with vulnerability speech.[233] In particular, this situation may arise if an information security researcher sells an exploit, leveraging a vulnerability directly or indirectly to a foreign government, and that government subsequently uses the researcher's exploit to inflict harm to the United States and its citizens.[234]

Under the Alien Tort Statute the Mens Rea *Standard for Corporate Aiding and Abetting Is Knowledge*, 10 NW. U. J. INT'L HUM. RTS. 119 (2011).

[226] *See* 18 U.S.C. § 371 (2006); *see, e.g.*, R. Michael Cassidy & Gregory I. Massing, *The Model Penal Code's Wrong Turn: Renunciation as a Defense to Criminal Conspiracy*, 64 FLA. L. REV. 353 (2012); Julia N. Sarnoff, *Federal Criminal Conspiracy*, 48 AM. CRIM. L. REV. 663 (2011).

[227] For example, a company may allege that an employee who discloses the existence of a security vulnerability in a product and refers to proprietary information to prove the flaw's existence may be participating in a scheme to steal critical intellectual property for the benefit of a foreign competitor. *See* Recent Case, *Criminal Law—*United States v. Chung, *659 F.3d 815 (9th Cir. 2011)*, cert denied, *No. 11-1141, 2012 WL 929750 (U.S. Apr. 16, 2012)*, 125 HARV. L. REV. 2177, 2181–84 (2012) (advocating an "expansive" reading of the Act and characterizing, ominously for security researchers, cyberspace as a budding venue for economic espionage); Elizabeth A. Rowe, *Striking a Balance: When Should Trade-Secret Law Shield Disclosures to the Government?*, 96 IOWA L. REV. 791 (2011).

[228] *See, e.g.*, discussion of the Auernheimer case *supra* note 164.

[229] For a discussion of treason, see, for example, Kristen E. Eichensehr, *Treason in the Age of Terrorism: An Explanation and Evaluation of Treason's Return in Democratic States*, 42 VAND. J. TRANSNAT'L L. 1443, 1447–62 (2009).

[230] For example, if a zero-day exploit sold by a U.S. researcher is used by a foreign government against the United States, a treason prosecution of the researcher may arise. *See id.* at 1458–61.

[231] Some computer security experts construe the criminal prosecution of Andrew "Weev" Auernheimer to reflect such a dynamic. *See, e.g.*, Blaze, *supra* note 155.

[232] The Model Penal Code provides that an aider must have "the purpose of promoting or facilitating the commission of the offense." MODEL PENAL CODE § 2.06(3)(a) (1985).

[233] Intentionally absent from this list are intellectual property harms. DMCA anticircumvention provisions require congressional and judicial reexamination. I would argue that the harm is not in circumvention but in the unauthorized use of the underlying code. The flaws of the DMCA anticircumvention provisions are outside the scope of this Article. For another scholar's critique of the DMCA, see, for example, Rebecca Tushnet, *I Put You There: User-Generated Content and Anticircumvention*, 12 VAND. J. ENT. & TECH. L. 889, 906–12 (2010).

[234] Allegations currently exist on Twitter that U.S. security researchers are selling exploits to foreign governments, including China. *See, e.g.*, Andrew Auernheimer, *@rabite*, TWITTER (Aug. 4, 2012, 1:01 PM), https://twitter.com/rabite/status/231842389382295553 ("I don't think exploit control

Finally, another pressing reason for the United States to clarify its position on vulnerability speech and informational speech in general relates to a looming international extradition and dual criminality problem. The extent of protection offered to U.S. researchers by the First Amendment likely conflicts with currently emerging law on vulnerability research in other countries.[235] As a consequence, in the future, U.S. researchers may be arrested when they travel or work abroad because of their research—research legal in the United States but potentially illegal in other countries.

CONCLUSION

This Article has presented a novel First Amendment approach to instructional or informational speech—the repurposed speech scale—through using the case study of vulnerability speech. The repurposed speech scale examines four factors in order to synthetically create an objective determination of a speaker's communicative intent in informational speech—the speaker's subjective goal behind the informational speech, the reputation of the forum selected for the speech, the degree of scarcity of the contributed information, and the extent of

mandates legislation but we shouldn't act as if @daveaitel sellin [sic] exploits to the Chinese is anything but vile[.]").

[235] The First Amendment provides U.S. citizens stronger free speech protections than the average level of protection granted by EU member state constitutions. Recently, legislative proposals in the Council of Europe have indicated an interest in criminalizing certain forms of security vulnerability research, specifically research done without the consent of a code's author. *See* Katitza Rodriguez & Marcia Hofmann, *Coders' Rights at Risk in the European Parliament*, ELECTRONIC FRONTIER FOUNDATION DEEPLINKS BLOG (June 20, 2012), https://www.eff.org/deeplinks/2012/06/eff-european-parliament-directive-attack-information-systems. The social policy reasons articulated in the previous section dictate that most security vulnerability research be protected and encouraged in the United States. As such, without a doctrinally coherent and thoughtful position on questions of vulnerability speech from the courts, it is possible that U.S. citizens engaging in vulnerability research entirely lawful in the United States may end up wrongly facing criminal prosecution in the European Union. *See* Rebecca Bowe, *Note to European Parliament: Let Security Researches Do Their Thing, Reap Public Benefits*, ELECTRONIC FRONTIER FOUNDATION DEEPLINKS BLOG (June 25, 2012), https://www.eff.org/deeplinks/2012/06/note-european-parliament-let-security-researchers-do-their-thing-reap-public. Particularly because the United States is adopting an aggressive stance in requesting extradition of U.K. nationals who have been linked to allegedly copyright infringing materials, it is likely that the U.K. and EU will expect reciprocity in extradition. In this way, a scenario could arise that reflects an inversion of the facts in *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002). In that case, a Russian citizen employed by a Russian company, Dmitry Sklyarov, was arrested at a computer conference in the United States for allegedly violating the Digital Millennium Copyright Act—a law which did not have a corollary in Russia where he authored the code at issue. *See* Pretrial Diversion Agreement, United States v. Sklyarov, No. CR 01-20138 RMW, 2001 WL 34131404 (N.D. Cal. Dec. 13, 2001); *Adobe FAQ: ElcomSoft Legal Background*, ADOBE, http://www.adobe.com/aboutadobe/pressroom/pressreleases/200108/elcomsoftqa.html (last visited Mar. 21, 2013). For a discussion of recent U.S. extradition requests for criminal copyright infringement, see, for example, Nate Anderson, *Copyright Wars Heat Up: US Wins Extradition of College Kid from England*, ARS TECHNICA (Mar. 13, 2012, 12:00 PM), http://arstechnica.com/tech-policy/2012/03/copyright-wars-heat-up-us-wins-extradition-of-college-kid-from-england/.

reasonable risk mitigation by the speaker. Tallying these factors in order to determine a speaker's objective dominant communicative intent, in situations where that intent demonstrates a desire to contribute to discourse on topics of public concern, that speech warrants First Amendment protection. However, in situations where a speaker's dominant communicative intent tends to indicate a goal of contributing to criminality, the speech does not warrant First Amendment protection and, thus, can provide a basis for congressional regulation, criminal prosecution, and civil suit. The repurposed speech scale offers a judicial operationalization to balance national security interests with creating a robust marketplace of ideas in informational speech. The approach also eliminates the confusion arising from the early code speech cases where code speech in different physical formats was analyzed differently: the repurposed speech scale is a context-sensitive approach that is simultaneously technology neutral. Because of this technology neutrality, the repurposed speech scale also removes the thorny question of medium-specific analysis for instructional or informational speech, while avoiding technology exceptionalism.

In closing, let us return a final time to the story of Jack and the jackpot. Notably, the story is the epitome of successful vulnerability speech: a reasonable researcher found flaws that would hurt consumers, and he then interacted with a reasonable company to correct flaws in a manner that minimized likely harm. While on its face, Jack's conference presentation would have triggered concerns over whether the speech facilitates criminality and potentially falls outside the First Amendment, behind the scenes, Jack's conduct demonstrated that his motivations were demonstrably otherwise: he and his employer cooperated with the code's author to correct flaws that would inevitably harm (or might have even already harmed) consumers. Applying the analytical lens of the repurposed speech scale, Jack's vulnerability speech would squarely fall into protected territory. His express goal was to improve security in the ATM industry. He engaged in his vulnerability speech at leading information security conferences, which were covered extensively by the mainstream press. He possesses esoteric, specialized knowledge regarding the craft of information security that led him to the discovery of the vulnerabilities, which he shared with the public. Finally, he engaged in reasonable risk mitigation strategies by cooperating with the ATM company as they patched the vulnerable code prior to his vulnerability speech, conscious that not only would his speech occur on a stage in Las Vegas, but also reside on YouTube in perpetuity. What happens in Vegas never stays in Vegas in the world of information security.