Journal of Criminal Law and Criminology

Volume 105 | Issue 1 Article 3

Winter 2015

Technology and the Guilty Mind: When Do Technology Providers Become Criminal Accomplices

Benton Martin

Jeremiah Newhall

0091-4169/15/10501-0095
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 105, No. 1
 Printed in U.S.A.

TECHNOLOGY AND THE GUILTY MIND: WHEN DO TECHNOLOGY PROVIDERS BECOME CRIMINAL ACCOMPLICES?

BENTON MARTIN* &

JEREMIAH NEWHALL**

The creators of today's most successful technologies share an important willingness to push the envelope—a drive that propels digital industry forward. This same drive, however, can lead some technology purveyors to push the limits of legality or even become scofflaws in their pursuit of innovation or (more often) profit. The United States must figure out how to harness the important creative force at the heart of the hacker ethic while still deterring destructive criminal wrongdoers. Because it is often courts that must answer this question, it is essential to examine the legal doctrines prosecutors use to sweep up technology providers.

This Article focuses on one type of criminal liability—accomplice liability—that can act as a dragnet on providers of technology that lends itself to criminal use. In particular, a violation of the federal statute for aiding and abetting, 18 U.S.C. § 2, can be implied in every charge for a federal substantive offense, and there is a potentially troubling strain of cases holding that knowing assistance can be enough to deem someone an aider and abettor, even without stronger evidence of a shared criminal purpose.

This Article examines when the proprietors of technology with criminal uses aid and abet their users' crimes. The aim is to help courts,

* Attorney with the Federal Defender's Office in Detroit, Michigan. He is grateful for helpful comments from Nate Anderson at *Ars Technica* and Professor Kay Levine at Emory Law School, as well as the excellent work of the editors of this journal.

** Public defender in Grafton County, New Hampshire. I join Benton in thanking Prof. Levine for her generous and insightful comments that helped shape subsequent drafts of this article. Thanks also to Bobby Murphy, Jenni Held, Hannah Lonky, Carolyn Hill, Sarah Halbach, Angela Koo, Peter Bloom, Jarrett Burks, Sunny Chang, Wade Formo, and Hannah Henkel for aiding and abetting the authors. You all have bright futures ahead. And thanks most especially to Karina Newhall, my constant accomplice.

prosecutors, and technologists draw the line between joining a criminal enterprise and merely providing technology with criminal uses. This Article explains the legal doctrines underlying this type of liability and provides examples of at-risk technologies, including spam software, file-sharing services, and anonymity networks like Tor. Ultimately, this Article concludes that the web of superficially conflicting rulings on the required mental state for aiding and abetting are best harmonized—and future rulings on liability for new technologies are best predicted—by looking to the existence of "substantial unoffending uses" for the product or service provided by the accused technologist.

TABLE OF CONTENTS

INTRODUCTION

Doctor Samuel Mudd awoke at four in the morning to find a patient at his door with a broken leg.[1] After Mudd took the man inside his home, he set and bandaged the leg. Lacking proper materials for a splint, Mudd broke apart his own bandbox (a thin wooden box for clothes), and then sent for a carpenter to make a pair of crutches.[2] Mudd's patient left within a day, and the two never met again. But within weeks, Mudd was arrested and then convicted of treason,[3] all for doing what doctors have always done: treating a patient in agony who came to his home in the middle of the night. This patient, however, had been John Wilkes Booth, and he had broken his leg in his flight from authorities after assassinating President Lincoln.[4]

Just as doctors think of themselves as neutral parties—helping cops and criminals alike—today's digital technology pioneers see themselves as neutral parties distributing their wares without partisanship. "A common hacker refrain," journalist Brendan Koerner writes, "is that technology is always morally neutral. The culture's libertarian ethos holds that creators shouldn't be faulted if someone uses their gadget or hunk of code to cause harm."[5] But innovation in the Internet age is so fast-paced (and generally messy) that legislators have scrambled to craft new punishments for new crimes, such as spam email and Internet hacking, further blurring the lines that separate innocent creators from criminal users.[6] When technology lends

---

[1] THE LIFE OF DR. SAMUEL A. MUDD 19 (Nettie Mudd ed., 1906) [hereinafter "LIFE OF MUDD"] (collecting original letters and documents).

[2] Statement of Dr. S.A. Mudd in the Matter of the Murder of the President, National Archives M-599, reel 5, frames 212–25, at 29–33 (1865).

[3] LIFE OF MUDD, *supra* note 1, at 19–20.

[4] *See id.* at 88–92 (arguments by Dr. Mudd's defense attorney about evidence of Mudd's and Booth's acquaintance). Dr. Mudd's attorney, Thomas Ewing, pointedly asked, as Dr. Mudd was accused of conspiring with Booth, whether breaking his own leg had been part of Booth's plan. *Id.* at 88.

[5] Brendan I. Koerner, *Alfred Anaya Put Secret Compartments in Cars. So the DEA Put Him in Prison*, WIRED (Mar. 19, 2013, 6:30 AM), http://www.wired.com/threatlevel/2013/03/alfred-anaya/all/, *archived at* http://perma.cc/G4VH-47GH; *see also* ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS 66 (2013) ("The central truth of the technology industry—that technology is neutral but people are not—will periodically be lost amid all the noise.").

[6] *See* Orin S. Kerr, *Foreword: Accounting for Technological Change*, 36 HARV. J.L. & PUB. POL'Y 403, 403 (2013). As Kerr noted:

> Changing technology presents a recurring problem for lawmakers. Laws are enacted with a background understanding of the facts. When those facts change, the effect of the old legal rules can change along with them. A law created for one world may have a very different impact when applied to the facts of a different era. As a result, changing technology and social practice often trigger a need for legal adaptation. Maintaining the function of old rules can require changing

itself to illegal use, courts must sort out the creators' criminal culpability: whether a cyberlocker's CEO is guilty of copyright infringement,[7] whether the creator of an anonymous online marketplace violated drug laws,[8] or whether software programmers should be jailed for enabling spam.[9] As Dr. Mudd learned, criminal law sometimes requires citizens to take sides, lest they be accused by the government of aiding and abetting criminals.

The scope of the federal statute for aiders and abettors, 18 U.S.C. § 2, is incredibly broad—it can be implied in every charge for a federal substantive offense[10]—and the notions of remoteness from the substantive criminal act used to limit the liability of criminal accessories are relatively untested in regard to Internet crime. Further, the Supreme Court in *Rosemond v. United States*, expressly left unresolved how § 2 applies to those who "incidentally facilitate a criminal venture" by providing a product or service, "knowing but not caring" about the principal's criminal intent.[11] The Court also arguably breathed new life into the strain of decisions holding that knowing assistance is enough to be an aider and abettor, even without stronger evidence of a shared criminal purpose.[12] Many accused technologists[13] try to exculpate themselves, with mixed success, by claiming ignorance of specific instances of their technology's criminal use. But unfortunately for today's technologists, the defense of lack of knowledge has dwindled in a world flooded with information.

This Article examines when the proprietors of technology with criminal uses aid and abet their users' crimes.[14] The aim is to help courts,

---

those rules to adapt to the new environment.

Id.

[7] *See generally* Benton Martin & Jeremiah Newhall, *Criminal Copyright Enforcement Against Filesharing Services*, 15 N.C. J.L. & TECH. 101 (2013) (analyzing charges of criminal copyright infringement against the cyberlocker Megaupload).

[8] *See* Superseding Indictment, United States v. Ulbricht, No. 14-cr-00068 (S.D.N.Y., Aug. 21, 2014), ECF No. 52.

[9] Press Release, U.S. Dep't of Justice, Virginia Software Writer Pleads Guilty to Aiding and Abetting Detroit Spam Conspiracy (July 7, 2009), *available at* http://www.justice.gov/opa/pr/2009/July/09-crm-664.html, *archived at* http://perma.cc/9UZ6-8RW8.

[10] *See, e.g.*, United States v. Armstrong, 909 F.2d 1238, 1241 (9th Cir. 1990).

[11] Rosemond v. United States, 134 S. Ct. 1240, 1249 n.8 (2014).

[12] *See id*. at 1248–49 (noting approvingly that the Court has found the requisite intent for aiding and abetting "when a person actively participates in a criminal venture with full knowledge of the circumstances constituting the charged offense").

[13] As used in this Article, the term "technologist" is intended to cover a wide variety of actors involved in developing, promoting, and managing the operation of technology.

[14] This Article grapples with the question left open by *Rosemond* and goes further to examine when proprietors of technology with both legal and illegal uses aid and abet their users' crimes. The question in *Rosemond* was limited to the merchant who knows but does

prosecutors, and technologists draw the line between joining a criminal enterprise and merely providing technology with criminal uses. Ultimately, this Article concludes that the web of superficially conflicting rulings on the required mental state for aiding and abetting are best harmonized—and future rulings on liability for new technologies best predicted—by looking to the existence of "substantial unoffending uses" for the product or service provided by the technologist accused of aiding and abetting.

I. THE HACKER ETHIC

To understand the mentality of technologists who skirt the edge of legality, it is worth returning to the dawn of the computer age, when the hacker ethic emerged with a distinctly anti-authoritarianism view of technology.[15] In the early 1960s, student programmers at Massachusetts Institute of Technology (MIT) developed a unique culture hailing the virtues of access to computer technology and freedom of information.[16] These early hackers believed deeply in their ability to improve life through computer technology, and they resented barriers and bureaucracies that hindered their hands-on exploration and betterment of the world around them.[17]

This mentality led to a veneration of decentralized experimentation and a certain willful blindness to what hackers saw as inefficient restrictions.[18] Ever mischievous, they probed flaws in MIT's phone system, ignored prohibitions on tampering with computer hardware, and intentionally crashed the school's million-dollar mainframe computers (to which they were allowed only limited access).[19] Adopting a unique concept of property rights, they would break into university labs to "borrow" components without ever considering it stealing, but would share their own

---

not care. This Article attempts to answer not only that question but also the (easier) question of what happens to a merchant who knows and does care that his wares facilitate crimes.

[15] *See generally*, STEVEN LEVY, HACKERS (2010) (tracing the history of the hacker ethic).

[16] *See id.* at 27.

[17] *Id.* at 28–31. These early hackers were, in many ways, like the early radio enthusiasts, who were comprised largely of tinkerers and hobbyists working without expectation of cashing in. *See* TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES 276 (2010) (observing that the homebrew computer hobbyists in California from which Steve Wozniak emerged "were the exact counterparts of the radio pioneers of the 1910s—hobbyists–idealists who loved to play with technology and dreamed it could make the world a better place").

[18] LEVY, *supra* note 15, at 28–119 (explaining at length the history of hackers' decentralized experimentation).

[19] *Id.* at 40–41, 88–89, 119.

software creations without thought to passwords, royalties, or licenses, repeating the mantra that "information should be free."[20]

As the computer revolution spread, so did the hacker ethic. Soon California computer enthusiasts, buoyed by an undercurrent of post-hippie activism, brought computers to the people by hacking hardware and sharing even proprietary software, like Atari's *Pong*.[21] As the market for personal computers grew, some programmers, like Bill Gates, were willing to profit from their creations.[22] Combined with this entrepreneurial spirit, the hacker ethic was eventually credited as inspiring the minds behind titans of the tech industry such as Microsoft, Google, and Facebook.[23]

The antiestablishment attitude persisted, too. For some, this outlook led to noble pursuits, leading them to forgo profiting on their achievements to innovate in the public interest. A good example is the early Internet pioneers protecting the nascent network against outside control by championing governance by consensus.[24] David Clark, the Internet's chief protocol architect for most of the 1980s, memorably remarked, "We reject: kings, presidents, and voting. We believe in: rough consensus and running code."[25] But this mentality also begot a certain lawlessness that would land

---

[20] *Id.* at 28, 46, 95–96, 98. Levy describes how some hackers went as far as taking correspondence courses in locksmithing to get special restricted blank keys or learned to duplicate high-security keys. *Id.* at 96. *See generally* THEODORE T. TOOL (A.K.A. TED THE TOOL), MIT GUIDE TO LOCK PICKING (1991), *available at* http://www.lysator.liu.se/mit-guide/MITLockGuide.pdf, *archived at* http://perma.cc/WS85-VZ4N.

[21] LEVY, *supra* note 15, at 219, 227.

[22] LEVY, *supra* note 15, at 232–33 (describing Gates's strident criticism of hack "sharing" culture); *id.* at 466 (noting that Gates and others involved in the early days of the computer revolution became "rich, famous, and powerful . . . even if it meant in some ways veering from the Hacker True Way").

[23] In an afterword in the twenty-fifth anniversary edition of Steven Levy's *Hackers*, the author discusses how "the hacker mentality has been incorporated as a value" at Google, and how Ben Fried, Google's Chief Information Officer, showed him a dog-eared copy of his book and told him he "wouldn't be here today" if not for reading it. *Id.* at 464, 474. Levy also remarked that Bill Gates's "faith in hacking underscored all of his work, right down to his staffing decisions." *Id.* at 467. Finally, in an interview with Facebook founder Mark Zuckerberg, Zuckerberg told Levy that he wants his company "to be the place where the best hackers want to work." *Id.* at 475–76; *see also* Steven Levy, *Mark Zuckerberg on Facebook Home, Money, and the Future of Communication,* WIRED (Apr. 4, 2013, 3:30 PM), http://www.wired.com/magazine/2013/04/facebookqa/, *archived at* http://perma.cc/X62B-6C8W.

[24] DAVID G. POST does a good job of capturing the spirit of consensus that went into developing the early Internet in IN SEARCH OF JEFFERSON'S MOOSE: NOTES ON THE STATE OF CYBERSPACE 126–62 (2009). Another example is Richard Stallman's fervent evangelism of open-source software. *See* LEVY, *supra* note 15, at 450, 461.

[25] Paulina Borsook, *How Anarchy Works*, WIRED (Oct. 1995), http://www.wired.com/wired/archive/3.10/ietf.html, *archived at* http://perma.cc/45BP-KHQW.

next-generation hackers in court. It is under a general banner of hackerism, for example, that the online collective Anonymous carries out devastating cyber-attacks.[26] Other hacker progenies, info-libertarians like Aaron Swartz and Chelsea (Bradley) Manning, raised the ire of law enforcement by pushing the boundaries of "information should be free."[27] Eventually, the term "hacker" was marred with the connotation of "digital trespasser."[28]

This history showcases a key difficulty that courts must address: as a rule, technology is "dual use," deployable for both nefarious and virtuous ends. This tension is perhaps best exemplified by the Internet itself. Its benefits are clear: it enables anonymous speech, creativity, and encrypted digital communication, among many other things. But as noted by Nate Anderson, a chronicler of Internet crime, the "productive chaos" of the Internet that makes these benefits possible also "makes all sorts of

---

[26] Martin & Newhall, *supra* note 7, at 134–35 n.158 (chronicling the origins and history of Anonymous).

[27] Manning was sentenced to thirty-five years for leaking classified documents to WikiLeaks. Charlie Savage & Emmarie Huetteman, *Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files*, N.Y. TIMES, Aug. 22, 2013, at A1. Online chat logs received that she spoke of doing so because "information should be free." Evan Hansen, *Manning–Lamo Chat Logs Revealed*, WIRED (July 13, 2011, 3:40 PM), http://www.wired.com/threatlevel/2011/07/manning-lamo-logs/, *archived at* http://perma.cc/QK9Z-Z5PA. Swartz committed suicide after his arrest and prosecution under the Computer Fraud and Abuse Act for using a computer program to download academic articles from the online repository JSTOR, which prosecutors alleged he intended to distribute. Noam Cohen, *A Data Crusader, a Defendant and Now, a Cause*, N.Y. TIMES, Jan. 14, 2013, at A1; Elizabeth Day, *Aaron Swartz: Hacker, Genius . . . Martyr?*, THE GUARDIAN (June 1, 2013), http://www.theguardian.com/technology/2013/jun/02/aaron-swartz-hacker-genius-martyr-girlfriend-interview, *archived at* http://perma.cc/HX9C-FEAF. The controversy surrounding both of these situations underscores the often fine line between the hacker ethic and a crime.

[28] LEVY, *supra* note 15, at 456. Merriam-Webster today defines "hacker" alternatively as "an expert at programming and solving problems with a computer" or "a person who illegally gains access to and sometimes tampers with information in a computer system." *Hacker*, MERRIAM-WEBSTER DICTIONARY ONLINE, http://www.merriam-webster.com/dictionary/hacker (last visited Sept. 6, 2014), *archived at* http://perma.cc/CC86-DWWB. Some people in the current MIT community dispute the use of the term "hacker" as applying to people who break into computer systems, preferring to call these people "crackers." This group defines "hacker" as "someone who does some sort of interesting and creative work at a high intensity level," including "writing computer programs" but also "pulling a clever prank that amuses and delights everyone on campus." *See Frequently Asked Questions*, INTERESTING HACKS TO FASCINATE PEOPLE: THE MIT GALLERY OF HACKS, http://hacks.mit.edu/misc/faq.html (last visited Sept. 19, 2014), *archived at* http://perma.cc/C73D-XTHK. The hacker ethic has also spilled into the purview of crimes regarding non-digital technology: a recent article in *Wired Magazine* questioned the conviction of Alfred Anaya, a master technician of secret compartments in cars, for conspiracy in drug crimes, suggesting that Anaya's calculated blindness to his compartments' uses should have absolved him. Koerner, *supra* note 5.

unproductive chaos not just possible but unavoidable."[29] Thus, for the better part of two decades, courts and legislatures have been attempting to strike the proper balance between productive and unproductive chaos.

Before turning to how criminal law plays into this balance, it is worth mentioning that there was once a serious debate about whether government should regulate the Internet at all.[30] In the 1990s, staunch defenders of Internet freedom contended that governments should avoid the temptation of trying to prevent local harm by imposing rules on the digital realm. In an influential article, professors David Johnson and David Post argued that the Internet, with its disregard for "geographical boundaries," had thrown "the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign."[31]

By the late 2000s, however, as citizens moved more of their lives into the digital world, the case for government intervention grew stronger. In 2006, professors Tim Wu and Jack Goldsmith predicted in their book *Who Controls the Internet?* that borderless-Internet advocates had overlooked the extent to which the success of the Internet hinged "on something invisible but essential: public goods like criminal law, property rights, and contract enforcement provided by government."[32] Reflecting on these

---

[29] NATE ANDERSON, THE INTERNET POLICE: HOW CRIME WENT ONLINE, AND THE COPS FOLLOWED 243–44 (2013).

[30] One of the most prominent of the early debates was about how much Congress could regulate Internet pornography to protect minors. Congress initially tried to impose criminal sanctions on anyone who transmitted "obscene or indecent" materials to people under the age of eighteen. Communications Decency Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 133, 133–36, part of the Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56. In 1997, the Supreme Court concluded that the Communications Decency Act violated the First Amendment. Reno v. Am. Civil Liberties Union, 521 U.S. 844, 849 (1997).

[31] David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996). This view of the Internet was not merely an academic utopia. Johnson and Post's argument foresaw the creation of private Internet governing bodies, like the Internet Corporation for Assigned Names and Numbers, to which the United States ceded control of the Domain Name System in 1998. MEMORANDUM OF UNDERSTANDING BETWEEN THE U.S. DEPARTMENT OF COMMERCE AND INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS, http://www.icann.org/en/about/agreements/mou-jpa/icann-mou-25nov98-en.htm (last visited Sept. 6, 2014), *archived at* http://perma.cc/DLP6-ZG82?type=source. This view was also echoed by the Supreme Court, which affirmed the Third Circuit's rejection of the Communications Decency Act of 1996, an early attempt at Internet censorship, and explained that this "unique medium" known as "cyberspace" is "located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet." *Reno*, 521 U.S. at 851.

[32] JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 140 (2006).

thoughts in 2010, Wu summarized why he and Goldsmith were so confident that the Internet would succumb to regulation:

> Despite its virtual qualities, behind the concept of a global network were living human beings, blood and flesh. The human body's susceptibility to pain and imprisonment is a large part of what the nation–state bases its rule on, and that had not changed. We predicted that the nation's threat of physical force, otherwise known as laws, would therefore shape the Network as much as its founding ambitions.[33]

II. THE LIMITS OF NEUTRALITY

The government's ability to control the "flesh and blood" underlying the Internet is core to this Article. Although hackers regard laws regulating the Internet as an anathema, their careless disregard for the intersection of evolving and traditional legal limits could land some of our brightest minds in jail.[34]

At the same time, Internet crime is a very real threat, and creative anarchy offers scarce protection to the public against the grave danger from those who would do harm with the "neutral" tools developed by those same "brightest minds." The United States remains resolved to protect its citizens from online crime. President Obama, for example, in his 2013 State of the Union address, warned that the country must "face the rapidly growing threat from cyber-attacks," lest the nation "look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."[35]

---

[33] Tim Wu, *Is Internet Exceptionalism Dead?*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 179, 181 (Berin Szoka & Adam Marcus eds., 2010). For another thoughtful discussion of this topic, see Alex Kozinski & Josh Goldfoot, *A Declaration of the Dependence of Cyberspace*, 32 COLUM. J.L. & ARTS 365, 366 (2009) ("The dilemma that online law-breakers face is that their cyberspace crimes have real-life motives and fulfill real-life needs.").

[34] For example, consider a recent profile of the late Steve Jobs and his potential violation of various white-collar criminal laws, in which the author warns that "Jobs's conduct is a reminder that the difference between genius and potentially criminal behavior can be a fine line." James B. Stewart, *Defying Convention and Maybe the Law*, N.Y. TIMES, May 3, 2014, at B1.

[35] 113 CONG. REC. H443–44 (daily ed. Feb. 12, 2013) (remarks by President Obama in the State of the Union Address). Obama stated:

> America must also face the rapidly growing threat from cyber-attacks. (Applause.) Now, we know hackers steal people's identities and infiltrate private emails. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.

At the periphery of this brewing war between law enforcement and those who would use the Internet to do harm sit the "neutral" hackers and innovators. They wish to innovate, to create, and to invent—they do not want to takes sides in a struggle to regulate the Internet and enforce the law. Yet as discussed in this Part, technologists cannot sit idly while their technologies find criminal use, as the very act of not intervening pushes them closer to criminal culpability.

A. THE LEGAL AND MORAL AMBIGUITY OF INTERNET CRIME

In the wake of such dire threats from Internet crime, all of the foregoing discussion of the "Hacker Ethic" and the insistence on "neutrality" by avowed (albeit petty) criminals at such privileged havens as MIT sounds a bit bloodless. These self-dubbed "hackers," insisting on the neutrality of computer codes that can crash a power grid, echo the Holmesian bad man, who cares nothing for morality, but only for what the law prohibits.[36] For while most understand the need to deter the Holmesian bad man, few have any sympathy for him.[37]

Not all computer crime, however, lines up neatly with our moral compass. The same person who would circle back to the drive-through after receiving too much change may think nothing of uploading a copyrighted song.[38] The moral line demarcating taking someone else's money shines

---

Id.

[36] Oliver Wendell Holmes, Jr., *The Path of the Law*, 10 HARV. L. REV. 457, 459 (1897). Holmes stated:

> [A] bad man has as much reason as a good one for wishing to avoid an encounter with the public force, and therefore you can see the practical importance of the distinction between morality and law. A man who cares nothing for an ethical rule which is believed and practised by his neighbors is likely nevertheless to care a good deal to avoid being made to pay money, and will want to keep out of jail if he can.

Id.

[37] Consider that, in 2013, a Pew Research Center Study showed that the group Internet and smartphone users most wanted to avoid tracking their online activity was "hackers" and "criminals," which beat out advertisers, harassing individuals, employers, and law enforcement. Lee Rainie, et al., *Anonymity, Privacy, and Security Online*, PEW RESEARCH CENTER (Sept. 5, 2013), http://pewinternet.org/Reports/2013/Anonymity-online.aspx, *archived at* http://perma.cc/S3TN-4U7W.

[38] Consider the anecdote about a young woman promised by a mysterious stranger that if she pushes a button she will receive $50,000, but that when she does, some person whom she has never known will be killed. *See* Richard Matheson, *Button, Button*, PLAYBOY, June 1970, at 131, 132 [hereinafter *Button* 1970]; *see also The Twilight Zone: Button, Button* (CBS television broadcast Mar. 7, 1986) [hereinafter *Button* 1986] (upping the ante to $200,000). The woman, desperate for money, succumbs and pushes the button, unable to care enough

bright, but the moral division between copying a short story published in 1922 and one published in 1923 remains evasive.[39] But practical necessity requires the law to draw lines that morality does not.[40] That is why, although the morality of sports gambling or prostitution may not shift with state lines, the legality of each does. These arbitrary lines become even more difficult to follow because of the complexity in determining jurisdiction in regard to business conducted via the Internet.[41] The most punctilious of technologists[42] would have difficulty knowing if, for example, his software to support online gambling were legal.[43]

So legal and moral ambiguities abound online, and not only for adherents to an anarchist Hacker creed, but for well-meaning technologists

---

for someone she will never know to refrain from causing their death. The televised version has the better ending: the stranger who brought the button pays the woman her blood money and then, as he leaves, promises that the next person who receives the button (and a similar offer) will be someone that the woman *has never met*. *See Button* 1986, *supra.* The tale wryly demonstrates the weak pull of human empathy when victim and victimizer remain anonymous to one another, even for victims of the most serious crimes. Internet criminals often never meet their victims (unless caught); they need only push a button.

[39] *See* Societe Civile Succession Guino v. Renoir, 549 F.3d 1182, 1189 (9th Cir. 2008). The court noted:

> The year 1923 is significant because the 1976 Act, which became effective on January 1, 1978, and the 1998 Copyright Extension Act, operate together to create a bright line rule for which works are now in the public domain: works published before January 1, 1923, are generally in the public domain.

Id.

[40] There is, of course, substantial scholarship on the relationship between morality and criminal regulation. For a critical discussion of modern views on the topic, see William J. Stuntz, *Self-Defeating Crimes*, 86 VA. L. REV. 1871 (2000).

[41] *See* Advanced Tactical Ordnance Sys., LLC v. Real Action Paintball, Inc., 751 F.3d 796, 802–03 (7th Cir. 2014) (questioning whether a website's interactivity can bestow jurisdiction); Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1123–25 (W.D. Pa. 1997) (creating test to determine jurisdiction over business conducted exclusively via Internet).

[42] What we might term the "Holmesian hacker" (after Holmes's bad man) or the "lawful neutral" hacker. *See* MIKE MCARTOR & F. WESLEY SCHNEIDER, COMPLETE SCOUNDREL: A PLAYER'S GUIDE TO TRICKERY AND INGENUITY 8–9 (2007) (explaining the concept of "lawful neutral" character alignment for Advanced Dungeons and Dragons edition 3.5).

[43] Consider the case against programmer Robert Stuart. In 2012, Stuart was indicted in New York for violating a state law against promoting gambling because his company sells online-sportsbook software. The software was licensed to companies who *in turn* licensed it to other companies for use in jurisdictions where sports gambling is legal, and Stuart swore himself that he never accepted any illegal bets at all, but New York State prosecuted him nonetheless after he refused to assist them by installing a "backdoor" in his software. *See* Kim Zetter, *Write Gambling Software, Go to Prison*, WIRED (Jan. 3, 2013, 6:30 AM), http://www.wired.com/threatlevel/2013/01/coder-charged-for-gambling-software/all/, *archived at* http://perma.cc/A9ZV-VVV3.

as well. When ambiguity allows the laws to sweep too broadly, they ensnare even those who meant to tread carefully within the lines of both law and morality.

Legal ambiguity also comes with an economic cost to society. A chief goal of criminal punishment is deterrence, but when the limits of forbidden conduct are unclear, the law deters too much, hobbling innovation that would be not only legal, but desirable.[44] Just as unclear rules for intellectual property stifle innovation,[45] so too an ambiguous line between guilt and innocence in aiding and abetting Internet crimes chills those who might otherwise have created the next Google or eBay.

This legal ambiguity reaches its height when deciding whether to prosecute creators of "dual use" technologies, by which we mean those inventions or services which may be used for good or ill. It is easy to decide the culpability of a "black hat" hacker who crashes a power grid, but harder to decide whether the creator of the program he used should share in that culpability. Yet the trend of pursuing the abettors of Internet criminals—sometimes in lieu of the principals—is in many ways unsurprising.[46] The sources of illegal goods are often located abroad or hidden through anonymizing software, so the government aims its enforcement efforts at intermediaries within (or arguably within) its jurisdiction.[47] The choice of criminal process is also predictable, for criminal law bestows sweeping powers on the federal prosecutor. In taking on file-sharing services, for instance, prosecutors have seized domain names, recorded internal computer conversations, sought extradition of overseas defendants, and wiped out data from innocent third parties as collateral damage.[48]

For technologists who see their role as neutral and insulated from their users' criminal activity, discerning the uncertain and shifting line between bystander and accomplice is paramount. But it is a line that exists inside the mind of the accused—the acts themselves are lawful. The would-be law-abider has no bright line to tell him when a legal act becomes a crime, and

---

[44] *See* Vance v. Rumsfeld, 701 F.3d 193, 210 (7th Cir. 2012) (Wood, J., concurring) ("Courts must balance the risk of over-deterrence against the public interest in deterrence of unlawful conduct." (citations and internal quotation marks omitted)).

[45] *See* Benton C. Martin, Comment, *The American Models of Technology Transfer: Contextualized Emulation by Developing Countries?*, 6 BUFF. INTELL. PROP. L.J. 101, 126 (2009) (discussing how overbroad patent protection stifles innovation with the threat of legal consequences).

[46] For examples, *see infra* Part IV.

[47] *See* GOLDSMITH & WU, *supra* note 32, at 68–77 (discussing how governments try to exert control over the Internet through local intermediaries).

[48] Martin & Newhall, *supra* note 7, at 144–51.

the prosecutor and jury often have only circumstantial evidence of the accused's intent or desire.

This is not a new problem, but one that the Internet has amplified. Over a century ago, each act committed by Dr. Mudd was ostensibly legal—even admirable—but it was the jury's belief in his guilty mind that condemned him. Today, the Internet exponentially multiplies the number of people that technologists may aid, and drapes their interactions with a layer of anonymity. Doctor Mudd aided a single man, but a "black hat" hacker can provide computer code for a virus or worm to thousands of people in dozens of countries without ever seeing their faces or knowing their names. Inventing a computer virus is no more a crime than setting a leg, yet when created with the intent to aid others in infecting computers, it is a federal offense.[49]

With Internet crime, therefore, society faces a peculiar difficulty in deterring the "bad man" when the same act may be legal one moment and illegal the next, all depending on what was in his mind. Of course, this problem is not peculiar to Internet crime, as shown by the Mudd anecdote discussed earlier, but the peculiar ambiguities of the Internet, with its blurred jurisdictional lines and sometimes arbitrary distinctions between crime and commerce, have muddied the mens rea requirement. These "thought crimes"—legal acts with an illegal mental state—have proved an enduring puzzle for the judiciary, but are essential to understanding the culpability of today's technologists.[50]

B. THE DIFFERENT TYPES OF "THOUGHT CRIMES"

In the taxonomy of crime, "thought crimes" consist of three phyla: attempt, aiding and abetting, and conspiracy. The second on this list, aiding and abetting, provides the most vexing problems for technologists and is the chief concern of this Article. But understanding why proof of intent to "aid and abet" should be such an intractable problem requires understanding the other "thought crimes" as well.

---

[49] *See* 18 U.S.C. § 1030 (2012).

[50] The term "thought crime" is used here without the derision sometimes aimed at the idea of punishing the guilty mind. It is entirely natural that an act may be criminal or innocent depending on its perpetrator's intent. As Holmes put it: "[E]ven a dog distinguishes between being stumbled over and being kicked." OLIVER WENDELL HOLMES, JR., THE COMMON LAW 7 (Mark DeWolfe Howe ed., Belknap Press, 1963) (1881). So, too, premeditated killing may be self-defense or it may be murder, and it all hangs on the defendant's desires. Moreover, the requirement of a guilty mind operates to restrict, rather than enlarge, the criminal law, by placing a high hurdle of proof before the prosecution. The difficulty for courts lies in how the government clears that hurdle.

Certainly thought alone, without action, cannot be criminal. But these three crimes are unique because the forbidden conduct is both incomplete and undefined—the criminal does not actually steal, for example, but conspires to steal, or aids someone who stole, or attempts to steal. Other crimes are defined as much by intent (mens rea), as by the completed act (actus reus). The "thought crimes," however, embrace an amorphous cloud of actus reus, a category of conduct too broad for definition. So long as the accused acts with the forbidden desires to conspire, to aid and abet, or to attempt, he is guilty whatever he does, however innocuous.

Consider a client with a mental defect that constantly causes him to desire to commit crimes. The client is conscious of the defect and able to change his behavior, but not his underlying desire. For most crimes, the advice to the client is to refrain from certain acts: he can never be convicted of murder if he does not cause a death; never convicted of robbery if he does not take someone else's property. But the thought crimes vex this client and his lawyer. Because of his guilty mind, he may be convicted of attempted murder even if no one dies; convicted of aiding and abetting robbery even if he never takes another's property.[51] This is because any "substantial" act, combined with a guilty mind, will complete the crimes of attempt or of aiding and abetting. The list of such acts is infinite; the client cannot be advised to avoid them all.[52] Of course there exists an infinite variety of ways to murder, but all of them share the definitive characteristic of the death of a human being. "Substantial" acts for conviction under attempt or under aiding and abetting have no such limiting principle. The problem is not their multiplicity but their amorphousness; they are defined by the criminal mens rea and nothing else. The guilty mind condemns our hypothetical client before he starts.

First and foremost of the three "thought crimes" is the crime of attempt, which couples most any act with a guilty mind. Attempt requires an intent to commit the crime attempted and a "substantial step," although the step itself may be an innocuous act. (Attempt's cousins are those crimes which couple a specific act with an intent to commit a further act—most commonly, possession of a controlled substance with intent to distribute.)

---

[51] He may, however, avoid conviction for conspiracy so long as he resolves to disagree with everyone he meets. But the distinction between thought and agreement is slight, particularly when agreement may be implied from other (noncriminal) acts.

[52] The existence of "insubstantial" acts does not render the number of "substantial" acts finite. An infinite set of numbers may be divided into subsets that retain the infinite characteristic, e.g., an infinite set of odd numbers and an infinite set of even numbers. So, too, infinite acts may be divided into endless subsets of "substantial" and "insubstantial" acts.

Even very dangerous acts may be legal with proper intent. For example, consider the facts of *United States v. Olsen*, in which Olsen was convicted of developing a biological agent to use as a weapon after admitting he produced ricin.[53] Ricin is a deadly toxin derived from the humble castor bean. Possession of ricin is illegal if the possessor has an intent to use ricin "as a weapon," or if possessed in "a quantity" inconsistent with peaceful purposes.[54] A person who possessed a very small amount of ricin, developed, as Olsen claimed, out of a morbid curiosity—i.e., to see whether he really could make castor beans into poison—would not be guilty under this statute.[55]

Second, under 18 U.S.C. § 2, a person is punishable as a principal if the person "aids, abets, counsels, commands, induces or procures" the offense or "willfully causes an act to be done which if directly performed by him or another would be an offense against the United States."[56] Section 2 applies to all federal crimes,[57] and we refer to this section with the familiar moniker of "aiding and abetting." This provision will be the main focus of later Parts of this Article.

Third, the crime of conspiracy to commit an offense is complete upon an agreement to commit an offense and the commission of some act in furtherance of the conspiracy—it is the crime of attempt by team-up.[58] Like § 2's prohibition on aiding and abetting, § 371 applies to conspiracies to commit any other federal crime.[59] But the requirement of an agreement dispels much (though not all) of the ambiguity hinted at earlier (and detailed below). To commit conspiracy, the conspirators must give voice to their intent by expressing their agreement with one another, and, in giving voice to their intent, they provide proof of their guilty minds.[60]

---

[53] *See* United States v. Olsen, 737 F.3d 625, 626 (9th Cir. 2013) (Kozinski, J., dissenting from denial of rehearing en banc).

[54] 18 U.S.C. § 175 (2012). The Supreme Court rejected as unconstitutional the application of another statute barring essentially the same activity, 18 U.S.C. § 229 (2012), in *Bond v. United States*, 134 S. Ct. 2077, 2083 (2014). But possession of ricin out of "morbid curiosity" would also not be a crime under § 229, even though that section on its face forbids possession of a chemical weapon (including ricin) for *any* purpose, because the definition of a "chemical weapon" excludes any chemical possessed for a "peaceful purpose." 18 U.S.C. § 229F.

[55] *See Olsen*, 737 F.3d at 629–30 (Kozinski, J., dissenting from denial of rehearing en banc). This Article returns to this example in its second half.

[56] 18 U.S.C. § 2 (2012).

[57] Nye & Nissen v. United States, 336 U.S. 613, 620 (1949).

[58] 18 U.S.C. § 371 (2012).

[59] *Id.*

[60] Not every conspiracy will be so clear-cut. Consider the case of Alfred Anaya, who

Ostensibly, it should make little difference whether to charge the defendant as a conspirator or an abettor, because both are punished for even a minor role in the crime. The prosecution will often have its choice of how to charge a defendant (and for this reason may charge in the alternative), because the same conduct can make an accused a conspirator with a minor role or an abettor.[61] Consider what would be required for an exception—providing help to the principal without ever reaching an agreement. For example, if a person saw notorious bank robber John Dillinger in the act of robbing a bank and, hoping to aid him, tripped the security guard, that person would have committed aiding and abetting (because she acted with intent to help Dillinger commit a crime) but not conspiracy (because she had no agreement with Dillinger).[62]

Two important distinctions make the difference between conspiracy and aiding and abetting vital to prosecutors and defense attorneys. First, by a quirk of the hearsay rules, statements of a coconspirator are an exception to the hearsay rule, while statements of an abettor are not.[63] Second, the Supreme Court in *Pinkerton v. United States* held that every member of a conspiracy may be punished for the crimes of just one coconspirator, if the crime was reasonably foreseeable and committed in furtherance of the conspiracy.[64] This rule of liability is inapplicable to aiders and abettors who,

---

never expressly agreed to help anyone distribute narcotics. Koerner, *supra* note 5. Anaya's business was putting secret compartments into cars; the government charged that Anaya should have known that these compartments could have had but one purpose, and by providing these compartments he joined the conspiracy to distribute the narcotics squirreled therein. *Id.*

[61] *See* United States v. Ailsworth, 867 F. Supp. 980, 987 (D. Kan. 1994).

[62] "'There is no requirement that there be an agreement in order to convict of aiding and abetting. Conspiracy to commit a crime and aiding and abetting in its commission are distinct offenses.'" United States v. Palazzolo, 71 F.3d 1233, 1237 (6th Cir. 1995) (quoting United States v. Frazier, 880 F.2d 878, 886 (6th Cir. 1989)).

[63] FED. R. EVID. 801(d)(2)(E).

[64] Pinkerton v. United States, 328 U.S. 640, 647–48 (1946). The *Pinkerton* rule has faced opposition, and has decreased in use in recent years, because of due-process concerns arising when the conspirator and the crime are especially attenuated. Wayne R. LaFave described this opposition in *Substantive Criminal Law*:

> Although the *Pinkerton* rule never gained broad acceptance, the opposition to it has grown significantly in recent years. It was rejected by the draftsmen of the Model Penal Code and of the proposed new federal criminal code. Most of the state statutes on accomplice liability require more than membership in the conspiracy, and the language in these statutes has been relied upon by courts in rejecting the conclusion that complicity is coextensive with conspiracy. The rule continues to exist in the federal system, though the courts "are mindful of the potential due process limitations on the *Pinkerton* doctrine in cases involving attenuated relationships between the conspirator and the substantive crime." The same may be said of at least some of the states which still utilize the *Pinkerton* principle.

while liable for the crimes they aid to the same extent as the principal, are not liable for *all* of the principal's other crimes. These are a few of the advantages that make conspiracy charges, in the words of Learned Hand, the "darling of the modern prosecutor's nursery."[65]

Yet the government has much to gain by jettisoning a conspiracy charge in favor of charging aiding and abetting under § 2. The prosecution loses a hearsay exception[66] but no longer must prove an agreement.[67] To charge technology providers with reaching an *agreement* with anonymous clients scattered across our globe would be difficult, which makes aiding and abetting a better fit for these prosecutions. But with no express agreement, we come to the root of the dangerous ambiguity in the criminal law: how to know the defendant's mind.

C. PROOF OF "THOUGHT CRIMES" BY CIRCUMSTANTIAL EVIDENCE

Absent a confession, jurors and judges must decide the contents of a defendant's mind by circumstantial evidence. Occasionally, however, prosecutors discover nearly direct evidence of a defendant's mind, as with a diary or journal.

For an example of nearly direct evidence of intent, consider *United States v. Olsen*, wherein Olsen claimed that he converted castor beans into ricin out of idle (though dark) curiosity, and not for use as a weapon.[68] If

---

WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 13.3(a) (2d ed. 2003) (footnotes omitted).

[65] Harrison v. United States, 7 F.2d 259, 263 (2d Cir. 1925) (Hand, J.) For one circuit judge's paean to the broad reach of conspiracy laws, see United States v. Hassan, 742 F.3d 104, 146 (4th Cir. 2014) ("Over the course of the modern legal era, the pursuit of federal conspiracy convictions has doubtlessly been a boon to United States Attorneys.").

[66] Actually, to the chagrin of defense attorneys across the country, the government may still claim the hearsay exception as it applies even to unindicted conspirators.

[67] Not having to prove an agreement can make a critical difference. As just one example, defendant Herbert Phipps challenged his conviction for conspiracy to contribute drugs on the grounds that he never agreed to join the drug ring; he was only a dealer. United States v. Moreland, 703 F.3d 976, 984 (7th Cir. 2012). The Seventh Circuit explained that selling was enough for aiding and abetting but not conspiracy:

> "[K]nowledge of a buyer's intention to commit a crime with a supplier's goods doesn't imply an agreement between the buyer and the seller that the buyer do so. That knowledge, coupled with the supplier's having supplied the buyer with the means (in this case a supply of drugs) of committing the illegal act of retailing an illegal drug, could make him an aider and abettor of the buyer's crime but not, without more, a conspirator with the buyer."

Id.

[68] *See* United States v. Olsen, 737 F.3d 625, 626 (9th Cir. 2013) (Kozinski, J., dissenting from denial of rehearing en banc).

that was true, then he was innocent, and so the government faced the challenge of proving what was in Olsen's head.[69] To do so, the government built a case on something very close to Olsen's actual thoughts—his Google searches. Olsen Googled such phrases on "undetectable poisons" and "untraceable death pill" (ricin is virtually undetectable in an autopsy).[70] Such a history comes close to showing Olsen's own thoughts—and suggests something very different than had he Googled "is ricin safe" or "how to do home experiments with ricin without hurting anyone." Moreover, given the scant uses to which ricin could be put *other* than homicide, Olsen's conviction is hardly a surprise. "Morbid curiosity" is not a substantial use for a deadly, undetectable, and banned poison, so the jury was not unreasonable when it inferred that Olsen's true intent was more nefarious.

With aiding and abetting, as with attempt, the ultimate evidence of guilt or innocence will be locked inside the defendant's mind, the one place where the government cannot place a wire, send a confidential informant, or recruit a cooperating witness. That is the battleground for trial, and likewise it is rightly the focus of challenges to sufficiency of the evidence on appeal. It is a rare case in which the defendants have made express their desire to violate the law, although it is somewhat more likely in cases of conspiracy, because remember that crime requires an agreement to commit another crime.[71] Because intent, or desire, which is sometimes called "specific intent," can usually be shown only by inference, prosecutors ask the jury to infer intent from circumstantial evidence of the abettor's acts and his knowledge of the actions of others.

III. SHIFTING DEFINITIONS OF THE GUILTY MIND OF AIDERS AND ABETTORS

Because of the flexibility required in aiding-and-abetting cases, writing an all-encompassing set of rules for courts to apply to aiding-and-abetting law would be a bootless errand. This Part attempts a more modest goal: an

---

[69] *Id.*

[70] *Id.* at 629; United States v. Olsen, 704 F.3d 1172, 1186 (9th Cir. 2013).

[71] For example, in a memorable scene from *The Informant*, a confidential informant for the FBI prodded several corporate executives, who were reaching a tacit but unspoken agreement to illegally fix lysine prices, into making their agreement explicit while they were being secretly videotaped. The informant feigns misunderstanding, asking: "What are we doing here?" He then leads the group in saying, in unison, that "we are all agreeing" to fix the price of lysine. *See* THE INFORMANT! (Warner Bros. 2009); *see also* KURT EICHENWALD, THE INFORMANT (2000). But because aiding and abetting does not require agreement, such smoking gun evidence of desire to aid the crime is rare.

analysis that describes what courts *are* doing by revealing a logical through-line connecting seemingly inconsistent decisions about aiding and abetting. Any common thread also serves as a predictive rule, foreshadowing how courts will apply the law of aiding and abetting to future technologies.

This Article does not seek to champion new normative rules for courts or legislatures to adopt. A court *could* adopt the "substantial unoffending uses" analysis proposed, but this Article's thesis is that such an adoption would be a cosmetic change rather than a substantive one. When legal scholars don their practitioner hats, they routinely predict for clients how a court will apply existing law to new facts. This Article provides a tool for that analysis, one that jives more consistently with the varied rulings than the partial and conflicting rationales espoused in legal opinions. Like pornography, courts know aiding and abetting "when [they] see it,"[72] as showcased by the Supreme Court's recent decision in *Rosemond*.[73] This Article's "substantial unoffending uses" analysis describes *what* courts are seeing.

A. BACKGROUND ON AIDING AND ABETTING

It was only around the turn of the twentieth century that the law of aiding and abetting in the United States evolved to, as a rule, punish accessories as principals.[74] Before that time, the common law made fine distinctions between principals and accessories in felony cases (largely because, at one time, all felony offenders faced the death penalty, from which courts wished to shield accessories).[75] But as the Supreme Court explained when reviewing this history, in the painstaking process of defining these distinctions, "justice all too frequently was defeated."[76] If, for instance, the proceedings against the principal somehow faltered—say, the principal died or remained on the lam—the accessory escaped conviction as well.[77] Therefore, a reform movement mounted, and first England's Parliament, then state legislatures in the United States, and eventually the federal government, replaced judge-made law with statutes designed to

---

[72] Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

[73] Rosemond v. United States, 134 S. Ct. 1240, 1249 n.8 (2014). *See infra* notes 138–146 and accompanying text.

[74] Congress enacted penal codes to this effect in 1899 for Alaska and in 1901 for the District of Columbia; Section 2 was enacted in 1909. Standefer v. United States, 447 U.S. 10, 16–18 (1980).

[75] *Id.* at 15; *see* Robert Weisberg, *Reappraising Complicity*, 4 BUFF. CRIM. L. REV. 217, 223 (2000).

[76] *Standefer*, 447 U.S. at 16.

[77] *Id.* at 19–20 (discussing the House and Senate Committee Reports related to § 2).

punish accessories as principals.[78] The statutory language drafted at that time remains in effect today in the form of § 2(a).[79]

This rule finds its easiest application when there is clear evidence of a desire to assist in committing the underlying act. Absent an admission, however, proving desire to further criminal activity is a difficult endeavor, as illustrated by Dr. Mudd's assistance of John Wilkes Booth. Mudd's facially innocent acts transform once it is revealed that Booth met with Mudd before the assassination, that he stored supplies in Mudd's house, and that both Mudd and Booth were staunch supporters of the Confederacy; facts confirmed by another one of Booth's admitted conspirators.[80] The jury's decision to convict Dr. Mudd seems less mysterious in light of these facts, but Mudd never confessed, and some historians still believe in his innocence.[81] In Dr. Mudd's case, as in so many others, courts and juries are often asked to infer intent from evidence showing how much the accused knew about or assisted the criminal enterprise.

In making such inferences, courts draw on Judge Learned Hand's analysis from more than seventy-five years ago in *United States v. Peoni*,[82] which the Supreme Court adopted in 1949 in *Nye & Nissen v. United States*,[83] and reaffirmed in 2014 in *Rosemond*.[84] Peoni, a counterfeiter, put fake bills into circulation, and they passed through an intermediary to Dorsey, who was charged with possessing them. Peoni was charged as

---

[78] *Id.* at 16–18.

[79] The statute was originally identified in 1909 as 18 U.S.C. § 550, which became § 2(a) in 1948. 18 U.S.C. § 2(a) (2012) (based on 18 U.S.C. § 550 (1909)). At the same time, § 2(b) was added to punish "causers," defined as "[w]hoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal." *See generally* U.S. DEP'T OF JUSTICE, TITLE 9: U.S. ATTORNEYS' CRIMINAL RESOURCE MANUAL, § 2472, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm02472.htm, *archived at* http://perma.cc/G8NE-6JC2. This Article will not directly address this section, which has prompted its own body of case law, *see, e.g.*, Pereira v. United States, 347 U.S. 1 (1954), because the authors consider subsection (b) less likely than subsection (a) to be used against "dual use" technologies.

[80] *See* LIFE OF MUDD, *supra* note 1, at 66–84 (arguments by Dr. Mudd's defense attorney about evidence of Mudd's and Booth's acquaintance).

[81] *See, e.g.*, Frank J. Williams, *The Lincoln Assassination in Law and Lore*, *in* THE LINCOLN ASSASSINATION 137, 140 (Harold Holzer et al. eds., 2010). The Michigan legislature, at the urging of Dr. Mudd's grandson, passed a resolution declaring that "[h]istory has subsequently revealed" that Dr. Mudd was an innocent victim. *Id.*

[82] United States v. Peoni, 100 F.2d 401, 402 (2d Cir. 1938).

[83] Nye & Nissen v. United States, 336 U.S. 613, 619 (1949).

[84] Rosemond v. United States, 134 S. Ct. 1240, 1248 (2014) (referring to the *Peoni* standard as the "canonical formulation of [the] needed state of mind" for aiding and abetting liability).

Dorsey's accessory, but the conviction did not stand. Judge Hand concluded that to be guilty as an accessory, a defendant must "in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed."[85] He added that the words used to describe accomplice liability—"even the most colorless, 'abet'—carry an implication of purposive attitude towards it."[86] Under this rubric, the Second Circuit concluded Peoni could not be considered an accessory to Dorsey's crime because his connection to the endeavor ended once he was paid by the intermediary.[87]

The crux of the problem that Learned Hand squashed in *Peoni* was double-counting. When a transaction is the crime, whether that be passing counterfeit dollars or selling drugs, deeming buyer and seller as accomplices doubles their liability and, more crucially, destroys any difference in culpability.[88] If each side of a transaction is an accomplice to the other, and is thus punishable as principal, then junkie and juicer alike must answer for both the purchase *and* the sale. Congress did not intend for that type of twofold liability, which in essence eliminates different levels of culpability for the different sides of various transactional crimes.[89] Of course, not every drug buyer is a junkie; one dealer may sell to another, as a wholesaler to a retailer. But the punishments for quantity of drugs sold or possessed presume resale, for that is the justification for their enhanced penalty. Making every wholesaler an accomplice to every future sale would also be double-counting.

---

[85] *Peoni*, 100 F.2d at 402.

[86] *Id.*

[87] *Id.* at 402–03.

[88] The transactional crimes at issue are sometimes dubbed "victimless" crimes, but only because the direct victims are themselves culpable. Compare pimps, illicit croupiers, drug dealers on the one hand with prostitutes, gamblers, and addicts on the other. Whether the crime is pimping, gambling, or drug sales, it takes two to tango—the crime cannot be complete without both parties. A robbery is not complete without a victim, yet of course the victim does not abet her own mugging. Drug addicts are not as blameless as the victim of a robbery, but they are less culpable than their dealers. For that reason, Congress enacted different penalties for the mere possession of drugs, without intent to distribute (i.e., an addict's crime), than for the distribution of drugs (i.e., a dealer's crime).

[89] *See* United States v. Swiderski, 548 F.2d 445, 451 (2d Cir. 1977). The court stated:

> We must reject the government's suggestion at oral argument that in such a case the principal would nevertheless be liable as an aider and abettor of the agent's distribution to him, since this would totally undermine the statutory scheme. Its effect would be to write out of the Act the offense of simple possession, since under such a theory every drug abuser would be liable for aiding and abetting the distribution which led to his own possession.

Id.

This type of double-counting works even greater injustice in counterfeit currency cases (like *Peoni*) than in drug cases, because a dollar, whether real or counterfeit, is never consumed. Unlike a drug or an apple or even an issue of a law review, the dollar exists only to be passed on, again and again, as a means of trade. If Peoni were accomplice to every passing of his counterfeit bills, his crimes might never end. And under the government's theory he would have been, for remember that § 2 also makes illegal acts done through another, regardless of that other person's mental state. Thus even when the bills reach innocent customers, Peoni would have committed the crime of circulating bills again each time they change hands, for he facilitated each (unknowing) passing by placing the counterfeit bills into commerce.

Judge Hand could have solved the double-counting problem by holding that if the transaction *itself* is the crime (e.g., prostitution or narcotics distribution), as opposed to a transaction in furtherance of some other crime (e.g., the sale of burglary tools or a murder for hire), then the deal itself does not constitute aiding and abetting. A buyer and seller would never be accomplices to one another based solely on the purchase or sale. That standard would have ended accomplice liability at the deal itself, not only for Peoni but for drug dealers, prostitutes, and illegal gamblers as well. Those who facilitate such deals would answer as accomplices, but only for that deal, and only as an accomplice to *one* party to the transaction, never to both.

That is the rule in conspiracy.[90] If two people, one a buyer and the other a seller, agree to a sale of cocaine, they have surely entered an agreement to commit a crime. But this agreement is *not* an agreement for purposes of conspiracy; absent some other agreement, such as a joint effort at distribution, agreeing to the sale itself is not enough.[91] This neat legal fiction that the parties to a sale of cocaine do not have an "agreement" for the sale of cocaine neatly constrains the punishments attendant to criminal conspiracies to truly joint enterprises. Had Judge Hand invented the same rule for accomplices as the courts would later craft for conspirators, the court would have reached the same result in *Peoni* without the residue that forces courts to sort "knowledge" from "desire." That subtle distinction—

---

[90] "When the sale of some commodity, such as illegal drugs, is the substantive crime, the sale agreement itself cannot be the conspiracy, for it has no separate criminal object." United States v. Lechuga, 994 F.2d 346, 349 (7th Cir. 1993) (en banc); *see also* United States v. Wexler, 522 F.3d 194, 208 (2d Cir. 2008); United States v. Dekle, 165 F.3d 826, 829–830 (11th Cir. 1999).

[91] *See Lechuga*, 994 F.2d at 349.

which exonerated Peoni even as it condemns others—has spawned a surprisingly resilient problem for jurists ever since.

For the *Peoni* analysis is not as clear-cut as it might sound. For example, in 2002, Baruch Weiss, then an Assistant U.S. Attorney in the Southern District of New York, published a detailed analysis of differing interpretations of *Peoni* among federal appellate courts.[92] Weiss described the "six different approaches to the question of an aider and abettor's mental state," ranging from "purposeful intent" to "knowledge is sufficient whenever coupled with a substantial act."[93] But these inconsistencies were not part of a traditional circuit split; decisions within the same circuits contradicted one another. Weiss particularly criticized the Second and Seventh Circuits for conflicting stances on the standard, fluctuating from case to case between requiring specific intent—i.e., purposeful desire to assist the crime—and requiring only assistance with knowledge of the criminal acts.[94] Knowledge had been sufficient before *Peoni*, and some courts still relied on that earlier analysis.[95] Weiss ultimately advocated for a "derivative approach," tying the mental state for an accomplice to that of the principal.[96]

But Weiss's analysis is too absolute, as is any approach "that requires too much conceptual formulism or notions of constructive intent."[97] Note that *Peoni* is loaded with the hedging words of a circumstances-based standard—"*in some sort* associate himself," and "an *implication* of purposive attitude." This ambiguity allows courts to blur the lines between knowing assistance and purposeful intent.

This blurring of the purpose and knowing-assistance standards was on full display in the Supreme Court's recent decision in *Rosemond*. In reaffirming *Peoni*, the Court also approvingly noted that it had "found [*Peoni*'s] intent requirement satisfied when a person actively participates in a criminal venture with *full knowledge* of the circumstances constituting the charged offense."[98] As Justice Alito explained in dissent, however, "[t]here is some tension" in the cases about purpose versus knowing assistance as

---

[92] Baruch Weiss, *What Were They Thinking?: The Mental States of the Aider and Abettor and the Causer Under Federal Law*, 70 FORDHAM L. REV. 1341, 1344–45 (2002).

[93] *Id.* at 1373–76.

[94] *Id.* at 1397–1407.

[95] *Id.* at 1401–07 (discussing and quoting United States v. Fountain, 768 F.2d 790 (7th Cir. 1985), *modified*, 777 F.2d 345 (7th Cir. 1985)).

[96] *Id.* at 1486–88.

[97] This is how professor Robert Weisberg describes attempts to define "intent as opposed to mere knowledge." Weisberg, *supra* note 75, at 245.

[98] Rosemond v. United States, 134 S. Ct. 1240, 1248–49 (2014) (emphasis added).

the mens rea for aiding and abetting, yet the majority "refers interchangeably to both of these tests and thus leaves our case law in the same, somewhat conflicted state that previously existed."[99] Appellate courts also have not described the standard for aiding and abetting with rigorous consistency, instead portraying aiding and abetting as covering a spectrum of activity, with a bystander's knowledge falling outside the scope of liability for most crimes, and liability escalating from there up to conclusive proof of a shared purpose.[100]

Perhaps the trickiest mental state between these two extremes is that of "knowing assistance." This is the mental state of which technology providers are often accused—i.e., that they knew their users were criminals and profited anyways.[101] Justice Alito wrote in *Rosemond* that, in his view, "the difference between acting purposefully (when that concept is properly understood) and acting knowingly is slight."[102] Because the difference is slight, and the concept of acting "purposefully" is so rarely properly understood, perhaps particularly by engineers and programmers (or even prosecutors), the law risks ensnaring technology providers. Thus, uncovering how courts treat the knowing assister is core to this Article.

Justice Alito was right, however, to note that the Court has done little to pin down the mental-state requirement for knowing assisters. Even Weiss, in his effort to create distinct categories for accomplice mental states, conceded that "the Supreme Court, at one time or another, has adopted the purposeful intent approach, the knowledge approach, and the derivative approach, and never really discarded any of them."[103] For example, in adopting *Peoni* in *Nye & Nissen*, the Court also cited *United States v. Dotterweich*,[104] which arguably takes a different approach. In *Dotterweich*, the Court upheld the conviction of the president of a company caught shipping misbranded drugs—a strict-liability crime—even without evidence that he knew about the shipments.[105] Weiss argues that *Dotterweich* embraces the derivative approach, applying strict liability to

---

[99] *Id.* at 1253 (Alito, J., dissenting).

[100] *See generally* WILLIAM J. STUNTZ, THE COLLAPSE OF AMERICAN CRIMINAL JUSTICE (2011). Some of this lack of clarity in the judicial analysis of aiding and abetting may reflect, as William Stuntz argues, that modern American criminal law focuses more on procedural protections for defendants than substantive limits on criminal law. *Id.* at 196.

[101] *See infra* Part IV for examples.

[102] *Rosemond*, 134 S. Ct. at 1253.

[103] Weiss, *supra* note 92, at 1468.

[104] United States v. Dotterweich, 320 U.S. 277 (1943).

[105] *Id.* at 278, 284–85.

the accomplice.[106] In the same breath, however, the Court confirmed the malleability of accomplice liability, warning in the end that it "would be mischievous futility" to attempt to create "a formula embracing the variety of conduct whereby persons may responsibly contribute in furthering a transaction forbidden by an Act of Congress."[107]

Further, although courts have generally accepted *Peoni*'s standard as governing after the Court adopted it in *Nye & Nissen*, the Court has not rejected earlier cases suggesting that knowledge of criminal purpose is enough in some cases.[108] One of those earlier cases, *Bozza v. United States* from 1947, is even cited approvingly by the majority in *Rosemond*.[109]

Before *Bozza*, the Court issued seemingly diametrically opposite decisions in the early 1940s that address when providers of goods or services may share the users' guilty mind. Although these cases address conspiracy, they have implications for the law of aiding and abetting as well. First, in *United States v. Falcone*, the Court rejected conspiracy charges against sellers of sugar, yeast, and cans who knew the products would be used in the production of illegal moonshine.[110] Three years later, in *Direct Sales Co. v. United States*, the Court swung the other way, upholding the conviction of a drug wholesaler for conspiracy to violate drug laws.[111] A leading state decision on aiding and abetting would later usefully summarize the distinction between these cases—and their takeaway point for purposes of aiders and abettors—as "that distributors of such dangerous products as drugs are required to exercise greater discrimination in the

---

[106] Weiss, *supra* note 92, at 1468.

[107] *Dotterweich,* 320 U.S. at 285.

[108] *See, e.g.*, Rosemond v. United States, 134 S. Ct. 1240, 1249 (2014) (citing Bozza v. United States, 330 U.S. 160, 165 (1947)); United States v. Fountain, 768 F.2d 790, 797–98 (7th Cir. 1985), *modified*, 777 F.2d 345 (7th Cir. 1985). The Court noted in *Fountain*:

> Under the older cases, illustrated by *Backun v. United States*, 112 F.2d 635, 636–37 (4th Cir. 1940), and *Bacon v. United States*, 127 F.2d 985, 987 (10th Cir. 1942), it was enough that the aider and abettor knew the principal's purpose. Although this is still the test in some states, after the Supreme Court in *Nye & Nissen v. United States*, 336 U.S. 613, 619 (1949), adopted Judge Learned Hand's test—that the aider and abettor "in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed"—it came to be generally accepted that the aider and abettor must share the principal's purpose in order to be guilty of violating 18 U.S.C. § 2, the federal aider and abettor statute.

Id. (citations omitted).

[109] *Rosemond*, 134 S. Ct. at 1249.

[110] United States v. Falcone, 311 U.S. 205, 208 n.1, 210–11 (1940).

[111] Direct Sales Co. v. United States, 319 U.S. 703, 714–15 (1943).

conduct of their business than are distributors of innocuous substances like sugar and yeast."[112]

Then in *Bozza*, the Court applied this same type of approach to aiding and abetting.[113] The decision upheld a man's conviction for aiding and abetting the operation of a secret distillery with intent to defraud the government of alcohol taxes.[114] The dissent insisted that the conviction could not be sustained absent evidence that the defendant somehow furthered or promoted the tax fraud specifically.[115] But the majority reasoned that the jury could properly find Bozza guilty by concluding "that a person who actively helps to operate a secret distillery knows that he is helping to violate Government revenue laws."[116] Indeed, the Court added, evading taxes "is a well known object of an illicit distillery. Doubtless few who ever worked in such a place, or even heard about one, would fail to understand the cry: 'The Revenuers are coming!'"[117] As discussed later, *Bozza* proves especially useful in discussing the potential liability of technology service providers.[118]

B. MODERN EXAMPLES OF AIDING AND ABETTING

Like the decisions already discussed, modern aiding-and-abetting analysis is flexible and circumstance-specific. Because of this, the best way to further tease out common threads is to examine examples and hypotheticals.

A good starting point is a favorite hypothetical of Judge Richard Posner,[119] derived from a real case in California,[120] illustrating why

---

[112] People v. Lauria, 59 Cal. Rptr. 628, 631 (Cal. Ct. App. 1967).

[113] *Bozza*, 330 U.S. at 164–65.

[114] *Id.* at 164–65.

[115] *Id.* at 167–68 (Douglas, J., dissenting).

[116] *Id.* at 165.

[117] *Id.*

[118] There are circuit court decisions in the same vein as *Bozza*. *See* Bacon v. United States, 127 F.2d 985, 987 (10th Cir. 1942); Backun v. United States, 112 F.2d 635, 636–37 (4th Cir. 1940).

[119] Judge Posner has used this analogy (using either a dress or an address book) in at least four criminal cases. *See* United States v. Colon, 549 F.3d 565, 571 (7th Cir. 2008) (drug crime); United States v. Zafiro, 945 F.2d 881, 887 (7th Cir. 1991), *aff'd*, 506 U.S. 534 (1993) (drug crime); United States v. Giovannetti, 919 F.2d 1223, 1227 (7th Cir. 1990) (illegal gambling); United States v. Fountain, 768 F.2d 790, 798 (7th Cir. 1985), *modified*, 777 F.2d 345 (7th Cir. 1985) (murder). He also has used it in regard to copyright law. *See In re* Aimster Copyright Litig., 334 F.3d 643, 651 (7th Cir. 2003).

[120] *See* People v. Lauria, 59 Cal. Rptr. 628, 630–35 (Cal. Ct. App. 1967). In *Lauria*, the court refused to allow the conviction of a man who provided telephone answering services to

knowledge alone is typically not enough to warrant punishment as an aider and abettor:

> Suppose you own and operate a store that sells women's clothing. Every month the same young woman buys a red dress from your store. You happen to know that she's a prostitute and wears the dress to signal her occupation to prospective customers. By selling her the dress at your normal price you assist her illegal activity, and probably you want the activity to succeed since if it fails she'll stop buying the dress and your income will be less. But you are not an aider and abettor of prostitution because if you refused to sell to her she would buy her red dress from another clothing store, one whose proprietor and staff didn't know her profession. So you're not *really* helping her or promoting prostitution, as you would be if you recommended customers to her in exchange for a commission.[121]

So too, Judge Posner reasoned, the typical buyer of cocaine does not join the sellers' conspiracy because the sellers could no doubt find other willing buyers.[122]

Other decisions clarify, however, that even after *Nye & Nissen*, knowledge plus some act of support *can* lead to liability as an aider and abettor. Contrast the red-dress hypo with the conviction of inmate Randy Gometz.[123] Another prisoner, Thomas Silverstein, twice convicted of killing other inmates, stopped next to Gometz's cell.[124] Gometz quickly pulled up his shirt to reveal a shank in his waistband, and Silverstein reached into Gometz's cell, grabbed the shank, and stabbed an escorting guard twenty-nine times.[125] Gometz was convicted of aiding and abetting the murder but challenged the sufficiency of the evidence to convict him on appeal.[126] Judge Posner, again writing for the court, noted that there remained some "support for relaxing the [purposeful-intent] requirement when the crime is particularly grave."[127] Thus, he continued, the jury properly convicted Gometz based on evidence that he "knew that Silverstein, given his history of prison murders, could have only one motive in drawing the shank and

---

a group of prostitutes. *Id.* at 630. The court concluded that "although proof of Lauria's knowledge of the criminal activities of his patrons was sufficient to charge him with that fact, there was insufficient evidence that he intended to further their criminal activities, and hence insufficient proof of his participation in a criminal conspiracy with his codefendants to further prostitution." *Id.* at 635.

121 *Colon*, 549 F.3d at 571 (internal citations omitted).

122 *Id.*

123 The facts of this example come from *United States v. Fountain*, 768 F.2d at 793.

124 *Id.*

125 *Id.*

126 *Id.* at 798.

127 *Id.*

that was to make a deadly assault."[128] Gometz, in this sense, calls to mind Bozza, whom the Supreme Court declared to be an accomplice to tax fraud because dodging taxes was the clear purpose of running a secret distillery.[129] The decision also reaffirms the idea that "distributors of such dangerous products,"[130] whether drugs or shanks, must use greater care than distributors of yeast or dresses.

To further see how this tension between knowledge and purpose plays out in a specific context, it is useful to look at cases involving people assisting drug dealers because—courtesy of the war on drugs—they serve as a microcosm of the law of aiding and abetting. The easiest case is when an assister admits acting with intent to help the venture to distribute drugs.[131] A harder question arises when the evidence shows mere knowledge, but intent remains ambiguous—a guilty finding requires more than mere knowledge of intended drug dealing.[132] On one hand, the act of simply being a passenger in the car driven to a drug deal, even with full knowledge of the destination, is not enough to support a guilty finding for aiding and abetting.[133] On the other hand, the accused's conduct in aid of the illicit enterprise need not be overwhelming; it is enough that a person knowingly drove a drug dealer to a pick-up location.[134] The difference between passenger and driver is superficially one of actus reus (i.e., being a passenger is passive while driving is active) and not of mens rea. But that

---

[128] *Id.* at 799.

[129] Bozza v. United States, 330 U.S. 160, 165 (1947).

[130] People v. Lauria, 59 Cal. Rptr. 628, 631 (Cal. Ct. App. 1967).

[131] *See, e.g.*, United States v. Blaylock, 421 F.3d 758, 773 (8th Cir. 2005) (upholding conviction of driver when there was evidence he admitted that the purpose of the trip was to purchase drugs and that he took a vacation with a dealer in order for the dealer to "set him up dealing illegal drugs").

[132] *See, e.g.*, United States v. Heras, 609 F.3d 101, 107 (2d Cir. 2010); United States v. Jones, 44 F.3d 860, 869 (10th Cir. 1995); United States v. Poston, 902 F.2d 90, 93 (D.C. Cir. 1990).

[133] *Compare* United States v. Diaz-Boyzo, 432 F.3d 1264, 1269 (11th Cir. 2005) ("Diaz-Boyzo's presence in Eustolio Villa-Gamino's truck, where Eustolio Villa-Gamino had drugs hidden in a beer box inside a white bag, is insufficient by itself to support his conviction."); United States v. Pena, 983 F.2d 71, 73 (6th Cir. 1993) ("Guilt by association with the driver of the car, the act of being a passenger in the car, is insufficient."); United States v. Sanchez-Mata, 925 F. 2d 1166, 1169 (9th Cir. 1991) ("Sanchez-Mata's presence as a passenger in the car cannot support an aiding and abetting theory."), *with* United States v. Santana, 524 F.3d 851, 855 (8th Cir. 2008) (finding sufficient evidence of aiding and abetting drug dealing when passenger knew the illegal purpose of the trip, was paid and had been paid for similar trip before, lied to officers, and had drugs on his person); *Diaz-Boyzo*, 432 F.3d at 1270 (finding sufficient evidence when passenger participated in multiple trips with drug dealer, may have observed drug delivery, and kept loaded gun in his lap during the delivery).

[134] *See, e.g.*, *Heras*, 609 F.3d at 107.

distinction would not explain why being a passenger in a car—with the intent to make the trip seem like a family vacation rather than a drug smuggling expedition—would be aiding and abetting despite involving the same conduct of "being a passenger in the car" that courts have found insufficient in other contexts.[135] Nor does it address why simply sitting at home can be aiding and abetting if the accused lived in a safe house in order to make the house appear occupied.[136] The distinction is what a reasonable jury infers from the act about the accused's desires, and the more passive the action, the less likely an inference of guilt.

It is no defense, however, that the assistance was not essential to the crime. Courts regularly uphold the conviction of middlemen who assisted only with the financial end of a drug deal, even though the exchange of cash is not an element of a drug offense.[137]

The Court's recent decision in *Rosemond* arises from a similar context. Rosemond traveled with two compatriots to a local park to conduct a drug deal.[138] When the deal went south, one of the three fired a handgun.[139] The government charged Rosemond in the alternative with (1) use of a firearm during a drug crime and (2) aiding and abetting that offense.[140] The jury convicted Rosemond of the firearm offense but did not indicate whether it

---

[135] *See* United States v. Figueroa, 682 F.3d 694, 696 (7th Cir. 2012). In *Figueroa*, the court reasoned:

> Figueroa paid for Cruz and his family to fly from Chicago to Texas, and doubtless the purpose of having Cruz drive with his family rather than alone was, by making his trip seem innocent, to reduce the likelihood of his being apprehended en route. The family members thus were outsiders involved in the drug enterprise.

Id.; *see also* WE'RE THE MILLERS (Warner Bros. 2013) (depicting a pot smuggler who recruits a fake "family" to travel with him in an effort to deflect suspicion while crossing the border).

[136] *See* United States v. Vasquez-Chan, 978 F.2d 546, 552 (9th Cir. 1992) ("The government claims that her role may have been to live at the house, give it a lived-in appearance, and guard the cocaine. Such a role, if established by probative evidence, would permit a conviction for possession as an aider and abetter."), *overruled by* United States v. Nevils, 598 F.3d 1158, 1167 (9th Cir. 2010).

[137] *See, e.g.*, United States v. Coady, 809 F.2d 119, 124 (1st Cir. 1987) ("[T]hough one need not covet cash to be guilty of a § 841(a)(1) distribution, one may certainly aid and abet such a distribution—'associate [oneself] with the venture . . . [so] that [one] seek[s] by [one's] action to make it succeed'—by facilitating the financial climax of the deal.") (alterations in original) (internal citation omitted) (quoting Nye & Nissen v. United States, 336 U.S. 613, 619 (1949)); United States v. Raper, 676 F.2d 841, 849 (D.C. Cir. 1982) ("Raper's acts, in apparently arranging the sale, receiving the money, and counselling Childs satisfied all the requirements under 18 U.S.C. § 2(a) for conviction as an aider or abettor.").

[138] Rosemond v. United States, 134 S. Ct. 1240, 1243 (2014).

[139] *Id*.

[140] *Id.*

found that he used the gun himself or had merely aided and abetted in its use.[141] The Court ultimately reversed Rosemond's conviction because the trial court had used a jury instruction that did not require him to have had prior knowledge that one of his compatriots brought a gun.[142] In doing so, the Court also settled a circuit split about whether someone can be guilty of aiding and abetting a crime based on aiding just one part of the crime and not every element.[143] For the Court, it was enough that Rosemond aided the drug dealing, for which the gun became a part (as long as he had knowledge of the gun's existence).

Interestingly, in two footnotes, the Court made a point to state that it was not taking a position on two important lingering issues about aiding and abetting law.[144] First, the Court noted that "[s]ome authorities suggest an exception to the general rule when another crime is the 'natural and probable consequence' of the crime the defendant intended to abet."[145] Second, and more important for the issue at hand, the Court stated that it was not dealing "with defendants who incidentally facilitate a criminal venture rather than actively participate in it," as with "the owner of a gun store who sells a firearm to a criminal, knowing but not caring how the gun will be used."[146] The Court's silence on this point leaves open the question of the liability of technologists who provide knowing assistance to criminal users.

C. WHEN IS KNOWING ASSISTANCE ENOUGH?

This discussion illustrates that courts, including the Supreme Court, have not spoken uniformly about the standard for determining the guilt of the knowing assister, the category most likely to ensnare technology providers. At first glance, this lack of uniformity could cause one to lament, as does William LaFave in his leading criminal law treatise, that the cases "are generally in a state of confusion."[147] On closer look, though, a through-line emerges among the differing standards: a "substantial unoffending uses" test. Before examining this test, however, consider three other proposals to harmonize the case law on aiding and abetting.

---

[141] *Id.* at 1244.

[142] *Id.* at 1251–52.

[143] *Id.* at 1246–48.

[144] *Id.* at 1248 n.7, 1249 n.8. Somewhat mysteriously, Justice Scalia joined the majority's opinions *except for* those two footnotes. *Id.* at 1242.

[145] *Id.* at 1248 n.7.

[146] *Id.* at 1249 n.8.

[147] LAFAVE, *supra* note 64, § 13.2(e).

First, consider the approach Judge Posner suggested with Gometz's shank, that knowledge is enough for major crimes. This approach reconciles some of the cases, LaFave observes, as the seriousness distinction explains why courts would impose liability "for knowing aid to a group planning the overthrow of the government or to one planning to burglarize a bank, but not for knowing aid to such crimes as gambling, prostitution, and unlawful sale of liquor."[148] Moreover, this distinction may be justified on policy grounds: it burdens merchants with the obligation of policing their customers only for the most serious crimes.[149] But it is hard to see this approach gaining real traction in today's courts, as judges are often loath to openly make policy decisions, such as the varying severity of different crimes.[150]

A second approach is to put a gloss of substantial facilitation on § 2. The draftsmen of the Model Penal Code originally recommended this approach, reasoning that it would protect vendors of readily available goods and peripheral bit players who may have acted with willful blindness.[151] But the American Law Institute rejected the draftsmen's suggestion in favor of the *Peoni* party line (the Code currently requires accomplices to share "the purpose of promoting or facilitating the commission of the offense").[152] LaFave suggests that the test was rejected because of "vagueness,"[153] but

---

[148] *Id.* § 13.2(d) (internal citations omitted).

[149] *See id.*; *cf.* United States v. Blankenship, 970 F.2d 283, 287 (7th Cir. 1992). In *Blankenship*, the court stated:

> Because a lessor almost inevitably knows his tenant's business, the imposition of a criminal penalty is likely to deter but not to raise the costs of legitimate transactions. A bookie needs a wire room; if the law deters landlords from providing space for these operations, it will substantially cut down on crime.

Id.

[150] For example, recall John Roberts comparing judges to umpires: "Umpires don't make the rules, they apply them. The role of an umpire and a judge is critical. They make sure everybody plays by the rules, but it is a limited role." *Confirmation Hearing on the Nomination of John G. Roberts, Jr. to Be Chief Justice of the United States: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 55 (2005) (statement of John G. Roberts, Jr.); *see also* United States v. Holcomb, 657 F.3d 445, 463 (7th Cir. 2011) (Posner, J., dissenting from denial of rehearing en banc) ("A few judges may think that Congress is omnicompetent; more pretend to think that—what they really think being that literal interpretation of statutes is necessary to save the nation from judicial tyranny." (emphasis omitted)).

[151] LAFAVE, *supra* note 64, § 13.2(d) (citing MODEL PENAL CODE § 2.06, cmt. at 318 n.58 (1985)). Note that the less-serious crimes in this example are also all transactional crimes, suggesting that the *Peoni* rule should really be an exception for transactional crimes alone.

[152] MODEL PENAL CODE § 2.06(3)(a).

[153] LAFAVE, *supra* note 64, § 13.2(d).

there is a better reason to discard it. The test focuses on the degree that the accomplice's act furthered the criminal enterprise, even though the helpfulness of a certain act may only truly be known by the principal offender, and thus the approach risks punishing people for acts far beyond any they could have anticipated.[154] In any event, it does not appear to accurately reflect varying decisions of federal appellate courts.

A third approach, perhaps the most popular among scholars, is "reconceiving accessorial liability as a species of *recklessness*."[155] For example, Larry Alexander argues "purpose and knowledge can be reduced to recklessness because, like recklessness, they exhibit the basic moral vice of insufficient concern for the interests of others."[156] Taking a similar approach, Daniel Yeager has argued that accomplice liability should turn on the extent the accused engaged in "excessive risk-taking."[157] Yet although the concepts of recklessness and risk-taking may be helpful in understanding why society would punish knowing assisters,[158] it is unlikely that federal courts will eschew the hoary requirements of knowledge and purpose anytime soon.

This Article posits a fourth approach, one examining the "substantial unoffending uses" of an accused's contributions, to describe what federal courts generally do when faced with knowing assistance. This approach differs from the "substantial facilitation" inquiry, because rather than focusing on the degree the accused's assistance helped the offender, it focuses on the degree that the assistance was susceptible to substantial unoffending uses (like the red dress) versus well-known criminal uses (like Bozza's still or Gometz's shank). The test finds its best use in regard to knowing and neutral defendants—when there is evidence the accused knew someone was a criminal but no evidence of a desire either to aid or to hinder them in their criminal acts. This approach also addresses the problem

---

[154] For a similar argument, see Joshua Dressler, *Reassessing the Theoretical Underpinnings of Accomplice Liability: New Solutions to an Old Problem*, 37 HASTINGS L.J. 91, 121–23 (1985), which criticizes the "substantial participation test" for leading to "morally inappropriate conclusions" by punishing people not "for their personal connection with the punishable harm, but for their decision to join the criminal enterprise."

[155] Weisberg, *supra* note 75, at 248 (emphasis in original). Professor Weisberg concludes that this approach "is a remarkable common denominator to [recent] scholarly efforts however much they otherwise differ." *Id.* at 247.

[156] Larry Alexander, *Insufficient Concern: A Unified Conception of Criminal Culpability*, 88 CALIF. L. REV. 931, 931 (2000).

[157] Daniel B. Yeager, *Dangerous Games and the Criminal Law*, 16 CRIM. JUST. ETHICS 3, 4, 10 (1997).

[158] *See* Weisberg, *supra* note 75, at 247–61 (examining the usefulness of the recklessness standard).

of "willful blindness" by examining whether the assistance at issue bespeaks principally one true purpose to the outside observer (or, one could say, the reasonable person), rather than the accused's subjective mindset.[159]

D. FURTHER EXPLANATION OF THE "SUBSTANTIAL UNOFFENDING USES" ANALYSIS

To clarify the "substantial unoffending uses" approach, allow one more hypothetical enlisting prolific bank robber John Dillinger. Dillinger stops at a convenience store across the street from the local bank and asks to buy gloves. If the clerk recognizes Dillinger from a wanted poster and, not caring who he is, sells him gloves, the clerk is not a criminal: the gloves, like the red dress, have substantial unoffending uses. Now suppose Dillinger asks for bullets. If the clerk does not recognize him and obliges, there is no crime: no law bans bullets, and no nominally legal act is chargeable as aiding and abetting if the accused had no knowledge they were aiding a criminal. But if the clerk sells the bullets—knowing that in Dillinger's hands they are, like Bozza's still, employable for chiefly one obvious, criminal purpose—then the clerk may be found guilty of aiding and abetting bank robbery, even if he swears that he did not share Dillinger's reprobate purpose. Finally, if Dillinger empties the gunpowder from the bullets and uses his gun's flintlock mechanism to burn down the bank,[160] the clerk is not punishable for arson; starting fires is not a well-known use for a bullet.

But just as a firearm is not a cigarette lighter,[161] a prison shank (also called a shiv) is not a bookmark. When, as in *Fountain*, a defendant equips a murderer with a shiv, the prosecution will have no trouble proving a desire to aid murder because a prison shiv has *no* unoffending uses. A prisoner's mere possession of such a weapon violates prison rules, and the crude stabbing implement admits but one, homicidal, use.[162]

---

[159] For a useful discussion of how courts and academics have responded to the problem of "willful blindness" in regard to accomplice liability, see *id.* at 255–61.

[160] For an animated image of a flintlock mechanism generating sparks, *see Flintlock Mechanism*, WIKIPEDIA, http://en.wikipedia.org/wiki/Flintlock_mechanism (last visited Sept. 22, 2014), *archived at* http://perma.cc/ZE5B-WLVV.

[161] A pistol may, however, be repurposed to such an end. *See* United States v. Dotson, 712 F.3d 369, 371 (7th Cir. 2013), *cert. denied*, 134 S. Ct. 238 (2013) (mem.).

[162] Gometz argued that Fountain might have wanted the shank "for purposes of intimidation, escape, or self-defense." United States v. Fountain, 768 F.2d 790, 798 (7th Cir. 1985), *modified on reh'g*, 777 F.2d 345 (7th Cir. 1985). All of these uses were also illegal, however, and it would be a stretch (though not an impossible one) even under the earlier bank robber hypothetical to argue for exoneration because you believed you were abetting a *different* crime by the same principal, even if it were a less-serious one. In any event, the

This idea is further underscored by tweaking the oft-cited hypothetical about a shopkeeper serving women of the night.[163] Consider that, instead of prostitution, the shopkeeper stands accused of abetting a murder, the same crime as in *Fountain*, by selling a dress. One night, the woman asks for a dress to wear while murdering her pimp. She wants a red dress because that will signal to the pimp that she is conducting business as usual and will permit her to get the drop on him. If the shopkeeper sells her the dress, charging his regular price and refraining from comment on her plan, he neither aids nor abets murder, and to hold otherwise would be to require anyone with knowledge of an impending murder to take action to stop it. The law cannot so deputize the whole world. The shopkeeper might have a moral obligation to dissuade the woman, but not a legal one.

The distinction lies in the type of aid provided and the uses to which it may be put. Even with perfect knowledge of the woman's scheme, by selling a dress the shopkeeper has not materially aided a murder. The dress has not only substantial unoffending uses, it has *exclusively* unoffending uses. Its substantive purpose is to clad the wearer's nakedness, not to kill. Our murderess does not need a particular red dress, one that only the shopkeeper possesses; any red dress will do, and in a pinch, the dress might be ochre or rust. Murder does not depend on what dress the killer wears.[164] No reasonable jury could convict a shopkeeper for providing a dress because even when the purchaser vows to commit murder whilst wearing it, the dress possesses substantial unoffending uses.

Several courts have observed that the sale of gasoline to someone who knew it would be used to make Molotov cocktails "for terroristic use" would be aiding and abetting.[165] But the sale of gasoline to the same customer, with the same avowed terroristic intentions, knowing that *this*

---

circumstances in *Fountain* made the other suggested purposes of the shiv sufficiently unlikely for a reasonable jury to convict. *Id.*

[163] *See* United States v. Colon, 549 F.3d 565, 571 (7th Cir. 2008); *In re* Aimster Copyright Litig., 334 F.3d 643, 651 (7th Cir. 2003); United States v. Zafiro, 945 F.2d 881, 887 (7th Cir. 1991), *aff'd*, 506 U.S. 534 (1993); United States v. Giovannetti, 919 F.2d 1223, 1227 (7th Cir. 1990); *Fountain*, 768 F.2d at 798.

[164] A point memorably made by Marisa Tomei in her Oscar-winning role as Mona Lisa Vito. In response to a question from her fiancé (portrayed by Joe Pesci) about what pants to wear for deer hunting, she responds: "Imagine you're a deer . . . . Bam! A [expletive] bullet rips off part of your head! Your brains are laying on the ground in little bloody pieces. Now I ask you: Would you give a [expletive] what kind of pants the son of a [expletive] who shot you was wearing?" *See* MY COUSIN VINNY (20th Century Fox 1992). *Contra* KISS, DRESSED TO KILL (Casablanca 1975).

[165] *E.g.*, *Fountain*, 768 F.2d at 798; People v. Lauria, 59 Cal. Rptr. 628, 634 (Cal. Ct. App. 1967).

fuel will go only to fill the gas tank of his truck would *not* be aiding and abetting.[166] Judge Posner has suggested that the distinction here is "essential" versus "trivial" aid.[167] But a better way to understand the same distinction is as one between offending and unoffending uses for the accused's goods or services. A waitress serving the fugitive Dr. Richard Kimble[168] in a restaurant would be found not guilty of aiding a fugitive (in the unlikely event she were even charged), whereas a waitress sneaking food out the back to Dr. Richard Kimble as he hides in the bushes would be charged and likely convicted. The acts in one sense are the same—providing food that helps keep a known fugitive alive. But they suggest different desires on the part of the waitress, with the first suggesting a desire to serve food to customers (a substantial unoffending use for any restaurant), and the second evidencing a desire, more than willful blindness, to aid a fugitive.

As will be discussed later, this comparison is particularly useful for crimes involving potentially "dual use" technology. Consider the case of Alfred Anaya, a savant at creating secret compartments for cars, who was convicted of conspiracy to distribute narcotics, even though he never expressly agreed to assist with his clientele's illegal endeavors.[169] If instead of a car, Anaya had installed a hidden holster in a red dress to conceal our murderess's weapon of choice, the addition of a secret pocket would make the use of the dress material to the plan. Although such a secret may have unoffending uses, whether in a dress or a car, once the compartment's content is known to be illicit, it has but one use. When technologists *know* that their work is put to but one, illicit use—the government, for example, presented evidence that Anaya was told to make his compartments fit a kilo of cocaine—their provision of that work may fairly infer a desire that it be put to that use.[170]

---

[166] It might transform the use if the gas station were particularly remote, such that refusing to sell the gas might actually frustrate the terrorist's travel plans. *Zafiro*, 945 F.2d at 887 (inference of desire to abet may be inferred from "essential assistance," but not "trivial" assistance); *Giovannetti*, 919 F.2d at 1227 (selling an address book is insufficient evidence of desire to abet prostitution because principal, "at an infinitesimal cost in added inconvenience, would simply shop for address books among stationers who did not know her trade").

[167] *See* cases cited *supra* note 166.

[168] Doctor Kimble is the titular fugitive in *The Fugitive* movie and television series. *See* THE FUGITIVE (Warner Bros. 1993); *The Fugitive* (ABC television series Sept. 17, 1963 to Aug. 29, 1967).

[169] *See* Koerner, *supra* note 5.

[170] *Cf. Fountain*, 768 F.2d at 797–98.

E. THE IMPORTANCE OF THE STANDARD OF REVIEW

One final point must be mentioned before addressing the culpability of today's technologists. The foregoing discussion establishes that the standard for mental culpability in aiding and abetting remains uncertain, not only between circuits but within circuits, and part of this uncertainty can be resolved by applying this Article's proposed "substantial unoffending uses" analysis. But not all of it. What remains of the seeming contradiction in these appellate decisions might be explained by understanding the nature of the appellate review.

In the appellate cases discussed in this Part, the appellants' challenges to their convictions for aiding and abetting were not facial challenges to the statute, nor were they challenges claiming that the indictment failed to allege a crime. They challenged the *sufficiency of the evidence* to support a conviction.[171]

In fact, appellants in particular challenge the sufficiency of the evidence of their *intent*. In a direct federal appeal, defendants rarely challenge as insufficient proof of their *actions* for two reasons. First, the nature of federal jurisdiction is that it is largely discretionary, and federal prosecutions thus follow extensive investigations and mountains of evidence of the defendant's conduct. Wiretaps, surveillance videos, confidential informants, and cooperating witnesses often leave little room for all but metaphysical doubt about a defendant's conduct. Second, because aiding and abetting deals almost exclusively with acts that, taken alone, are legal or even laudable, such as giving a ride to a friend or setting a broken leg, the defendant may have no reason to dispute his actions, only his motives for them.

The problem with appellate rulings about intent is that, because of the standard of review, they do a poor job of clarifying whether any particular piece of evidence is conclusive proof of a guilty mind. Appellate review of the sufficiency of the evidence of a jury verdict is one of extreme deference, and permits reversal only when no reasonable jury could convict.[172] The court must view the evidence in the light most favorable to the prosecution, drawing all inferences in its favor.[173] So when an appellate court upholds a

---

[171] *See, e.g.*, Bozza v. United States, 330 U.S. 160, 162 (1947); *Fountain*, 768 F.2d at 794.

[172] *See* Jackson v. Virginia, 443 U.S. 307, 319 (1979) ("[T]he relevant question is whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." (emphasis omitted)).

[173] *Id.*

conviction for aiding and abetting, that does not mean that the evidence is *per se* proof of the crime alleged, only that a jury *might* convict based on that evidence.[174] This deference to the jury and to the trial judge, who heard and saw the witnesses and thus could best gauge their credibility, requires that appellate courts uphold convictions for aiding and abetting based upon a wide range of evidence of the defendant's desires. The jury need only have sufficient proof to draw an inference of desire to aid a crime, viewed in the light most favorable to the prosecution. That standard will always allow some ambiguity in the application of aiding and abetting analysis.

IV. THE CRIMINAL CULPABILITY OF TECHNOLOGY PROVIDERS

The United States must figure out how to harness the important creative force at the heart of the hacker ethic while still deterring destructive criminal wrongdoers. Although this balance must be struck with the help of technologists, the business community, and legislatures, it is often courts, for better or for worse, which are left to decide how society will treat technologists whose creations lead to widespread criminal activity. The second half of this Article seeks to clarify the application of aiding and abetting to Internet crime by providing examples of how criminal proceedings may play out against dual-use technologies.[175]

There are many potential examples, but this Part will address three broad, overlapping categories of technologies with criminal uses. First, there is technology that, although technically capable of innocent uses, was clearly designed for use in crime, as exemplified by spam software. Second is technology where the intended purpose is not clear; it may well have been designed for legitimate use but is being used rampantly for illegal activity. The example here is file-sharing services: cyberlockers, bookmarking sites, linking sites, and the like. Finally, there are technologies designed for good—like anonymity software and tools for testing security flaws—that by their very nature are susceptible to criminal misuse.

---

[174] *Id.*

[175] Although vagueness in criminal law may at times be a virtue, there is a countervailing interest in clarity from the technology industry. *See* Paul Szynol, *Fuzzy Boundaries: The Potential Impact of Vague Secondary Liability Doctrines on Technology Innovation*, *in* THE NEXT DIGITAL DECADE, *supra* note 33, at 393, 395 ("Without clear guidance from the legal system, tech companies are forced to engage in a 'fingers crossed' product design process . . . . Such risk can dissuade even the most resolute investors from marketing their invention—and it can literally bankrupt the braver among them.").

A. TECHNOLOGY DESIGNED FOR ILLEGAL USE: SPAM EMAIL MARKETING SOFTWARE

In the early 2000s, Alan Ralsky and his son-in-law, Scott Bradley, made millions of dollars through their Internet business in the suburbs of Detroit, Michigan.[176] The problem was that their business relied on artificially inflating the price of thinly traded stock by sending unsolicited bulk emails, a.k.a. spam, misleadingly promoting the stock—a standard "pump and dump" scheme.[177] This behavior is prohibited by 18 U.S.C. § 1037, part of the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (the CAN-SPAM Act). Spam remains enticingly lucrative: in 2011, researchers hijacked a spam botnet—a network of computers infected with software surreptitiously allowing outside control—and concluded that the spammer in control could make about $7,000 per day.[178]

But what distinguishes the Ralsky case from other large-scale spam takedowns[179] is the wide net cast by the prosecution. After indicting Ralsky, Bradley, and nine other coconspirators, federal prosecutors expanded the case to include David Patton, a software programmer who sold the email marketing tools Ralsky used.[180] Patton was charged with aiding and abetting Ralsky's spam operation.[181] Facing jail time, Patton pleaded guilty,

---

[176] Press Release, U.S. Dep't of Justice, Detroit Spammer and Three Co-Conspirators Sentenced for Multi-Million Dollar E-mail Stock Fraud Scheme (Nov. 23, 2009), *available at* http://www.justice.gov/opa/pr/2009/November/09-crm-1275.html, *archived at* http://perma.cc/6HMY-SXTU.

[177] Nate Anderson, *"Godfather of Spam" Goes to Prison for Four Years*, ARS TECHNICA, (Nov. 24, 2009, 11:40 AM), http://arstechnica.com/tech-policy/2009/11/godfather-of-spam-goes-to-prison-for-four-years/, *archived at* http://perma.cc/BFK-2GTK.

[178] Julie Rehmeyer, *Equation: How Much Money Do Spammers Rake In?*, WIRED (Feb. 28, 2011, 12:00 PM), http://www.wired.com/magazine/2011/02/st_equation_spamprofits/, *archived at* http://perma.cc/GR3L-WNXE. A 2010 survey also found that 43% of all email users in North America and Western Europe having opened or accessed spam emails, with 11% having clicked on links contained in email that they suspected to be spam. IPSOS PUB. AFFAIRS, KEY FINDINGS OF THE 2010 MAAWG EMAIL SECURITY AWARENESS AND USAGE SURVEY (Mar. 2010), *available at* http://www.maawg.org/sites/maawg/files/news/2010_MAAWG-Consumer_Survey_Key_Findings.pdf, *archived at* http://perma.cc/DH53-LP4Z.

[179] The stories of the federal actions against Oleg Nikolaenko and Sanford "Spamford" Wallace are recounted in Chapters 6 and 7 of ANDERSON, *supra* note 29.

[180] Press Release, U.S. Dep't of Justice, Virginia Software Writer Pleads Guilty to Aiding and Abetting Detroit Spam Conspiracy (July 7, 2009), *available at* http://www.justice.gov/opa/pr/2009/July/09-crm-664.html, *archived at* http://perma.cc/C3C6-AHKA [hereinafter Patton Press Release].

[181] *Id.*

admitting that he designed his software to enable insertion of false information into email headers and the use of "proxy" computers to conceal an email's origin.[182] (Both of these activities are specifically prohibited by the CAN-SPAM Act.[183]) He also admitted that he sold his software to Ralsky knowing that it would be used to violate the CAN-SPAM Act, and that he continued to provide product support with the intent to assist the operation's illegal actions.[184] Patton ultimately received a sentence of one day in jail for aiding and abetting violations of § 1037.[185]

Because Patton's admissions as a whole provided a factual basis to sustain his guilty plea, the court never had an opportunity to comment on which of his actions may have alone supported his convictions. The case usefully illustrates, however, the potential levels of involvement a software developer may have with a criminal organization. Based on the cases discussed earlier, it is clear that Patton's admission to providing the software and ongoing support with intent to assist the spam operation made him guilty of aiding and abetting. But what remains unclear is whether it would have been enough that Patton sold the software knowing that Ralsky would use it to violate the law, or that he designed the software for that purpose.

These same questions are at the heart of any prosecution of computer programmers employed by criminal enterprises. A good recent example is the ongoing prosecution of Jerome O'Hara and George Perez, former programmers for infamous Ponzi schemer Bernie Madoff, who were indicted in 2010 and went to trial in 2014 for allegedly using their technical acumen to hide Madoff's long-running fraud.[186]

The answer to the second question—whether designing programs for illegal use is a criminal offense—is the easiest. Designing a tool for use in a particular crime and giving it to a known purveyor of that crime would, almost certainly, satisfy even the most stringent *Peoni* adherent. The act of design for indictable use implies purposive attitude and a desire to aid the crime's commission, and the provision to the known criminal is an act of association with the venture. It was likely similar reasoning that, in March 2014, led the jury in the case of Madoff's programmers, who had worked

---

[182] *Id.*

[183] 18 U.S.C. § 1037(a)(2)–(3) (2012).

[184] Patton Press Release, *supra* note 180.

[185] United States v. Patton, No. 07-cr-20627-12 (E.D. Mich. Nov. 25, 2009) (judgment as to David A. Patton).

[186] *See* Indictment, United States v. O'Hara, No. 10-cr-00228 (S.D.N.Y. Mar. 17, 2010), ECF No. 17.

for him for more than a decade, to find them guilty of conspiring to commit securities fraud.[187]

But the first question—whether the knowing sale of software capable of both legal and illegal use to a criminal is a criminal offense—is harder. If Patton's software enabled spamming, and he knew Ralsky's intent, then to determine Patton's guilt, the court must examine the range of the software's use and what Patton knew about Ralsky. If the software was broadly capable of legitimate marketing uses, even though Patton somehow knew Ralsky to be a spammer, then Patton, like the seller of the red dress, is innocent; he should not be expected to police the use of his software. But if the software is capable of chiefly one use, and it is spam, Patton is in danger of criminal punishment.

B. TECHNOLOGY OVERRUN WITH ILLEGAL USE: FILE-SHARING SERVICES

Thanks to robust efforts by media companies and lawmakers to prevent file-sharing,[188] many of the legal decisions addressing dual-use technology come from the world of copyright. In the early 1990s peer-to-peer file-sharing flourished, propelled by hacker-led services like Napster, and it took more than a decade for media companies to stomp them out through civil litigation.[189] Throughout this time, appellate courts were repeatedly forced to grapple with these services' common defense: that they could not be liable for the infringing acts of their users. The matter ultimately made its way to the Supreme Court, which rejected the services' argument in its 2005 decision in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd*.[190] Contributory, or "secondary," copyright infringers, the Court concluded, *are* liable, despite their technology's dual uses, because there was evidence their operators intended to "induce" infringement.[191]

---

[187] *See* Erik Larson, *Madoff Aides Convicted in $17.5 Billion Ponzi Trial After Decades Working for Firm*, BLOOMBERG, (Mar. 25, 2014, 4:00 PM), http://www.bloomberg.com/news/2014-03-24/madoff-aides-convicted-in-five-month-fraud-trial.html, *archived at* http://perma.cc/JM6J-GAR6.

[188] *See* Bill D. Herman, *A Political History of DRM and Related Copyright Debates, 1987–2012*, 14 YALE J.L. & TECH. 162 (2012) (tracing the history of the strong copyright coalition).

[189] *See, e.g.*, *In re* Aimster Copyright Litig., 334 F.3d 643, 645 (7th Cir. 2003); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1010–11 (9th Cir. 2001); *see also* ANDERSON, *supra* note 29, at 199–202 (documenting the history of this litigation).

[190] Metro-Goldwyn-Mayer Studios v. Grokster, Ltd., 545 U.S. 913 (2005).

[191] *Id.* at 913, 932–33, 938–39.

Such inducement, the Court observed, was shown by Grokster marketing to former Napster users and not creating stronger anti-infringement tools.[192]

The parallels between *Grokster*'s standard of intent to promote infringement and the aiding and abetting standard of "purposive attitude" are obvious. As Judge Posner puts it, aiding and abetting is "the criminal counterpart to contributory infringement."[193] It is unsurprising, then, that federal prosecutors recently sought to apply this newly anointed theory of secondary infringement in the criminal context through use of § 2.[194]

In 2011, the United States prosecuted the operators of NinjaVideo, a site collecting links to copyright-infringing files stored on a popular cyberlocker named Megaupload.[195] After the NinjaVideo prosecution ended in a series of plea deals,[196] the next step was logical: go after Megaupload, then the "13th most frequently visited website on the entire Internet."[197] In 2012, the company was indicted in the Eastern District of Virginia, where it rented servers, for aiding and abetting criminal copyright infringement.[198]

Although the Megaupload prosecution has stalled because of problems extraditing the company's flamboyant leader from New Zealand,[199] the case has attracted significant controversy over the scope of aiding and abetting copyright infringement.[200] Viewed in a certain light, the prosecution is a success even without a conviction. As Orin Kerr explains, the government's goal was clearly "to push and prod other companies to take copyright

---

[192] *Id.* at 938–39.

[193] *In re Aimster*, 334 F.3d at 651; *see also* Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 815 (9th Cir. 2007) (Kozinski, J., dissenting) (analogizing secondary copyright liability to driving someone to a crime).

[194] *See* Martin & Newhall, *supra* note 7, at 114–15.

[195] Timothy B. Lee, *How the Criminalization of Copyright Threatens Innovation and the Rule of Law*, *in* COPYRIGHT UNBALANCED: FROM INCENTIVE TO EXCESS 63–64 (Jerry Brito ed., 2012); Rob Fischer, *A Ninja in Our Sites,* AM. PROSPECT, Jan./Feb. 2012, at 27; David Kravets, *Megaupload Assisted U.S. Prosecution of Smaller File-Sharing Service*, WIRED (Nov. 20, 2012, 2:54 PM), http://www.wired.com/threatlevel/2012/11/megaupload-investigation-roots/, *archived at* http://perma.cc/5GSM-RA3B.

[196] Press Release, U.S. Dep't of Justice, Leader of NinjaVideo.net Website Sentenced to 22 Months in Prison for Criminal Copyright Conspiracy (Jan. 6, 2012), *available at* http://www.justice.gov/usao/vae/news/2012/01/20120106ninjavideonr.html, *archived at* http://perma.cc/DF2F-M65U.

[197] Indictment, United States v. Dotcom, No. 1:12-cr-00003 at 2 (E.D. Va. Feb. 16, 2012), ECF No. 34 [hereinafter Dotcom Indictment].

[198] *Id.* at 1, 18–19, 31 (citing 18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).

[199] The judge presiding over the Megaupload case commented that the service's operators "may never be extradited." United States v. Dotcom, No. 1:12-cr-00003, 2012 WL 4788433, at *2 n.6 (E.D. Va. Oct. 5, 2012) (order denying motion to dismiss the indictment).

[200] *See* Martin & Newhall, *supra* note 7, at 119 n.98.

infringement more seriously."[201] To that end, there is evidence that, after the government seized Megaupload's domain names, assets, and data on its servers, several smaller file-sharing services voluntarily shut down,[202] and movie studio revenues increased significantly.[203]

But whether the government's theory holds water—as with any question of aiding and abetting—depends on the government's ability to produce evidence of knowledge of and intent to further criminal activity. As to Megaupload, James Grimmelmann observes, "If proven at trial, there's easily enough in the indictment to prove criminal copyright infringement many times over."[204] Indeed, the government says it has evidence of admitted intent, quoting private conversations among Megaupload's top brass in which they discuss helping infringers.[205] The government also cites the company's repeated refusal to remove (as required by law) its profitable-but-infringing content after receiving notice of infringement.[206] If the government proves these allegations, it is hard to imagine a court deciding that the company's operators did not participate in infringement as something they wished to bring about.

The tougher question is for the future, when cases are brought against less egregious offenders. As Grimmelmann notes, "much of what the [Megaupload] indictment details are legitimate business strategies many websites use to increase their traffic and revenues: offering premium subscriptions, running ads, rewarding active users."[207] If the case never goes to trial, questions about which of these strategies are legal will linger. Some

---

[201] Philip S. Corwin, *MegaBust's MegaQuestions Cloud the Net's Future*, CIRCLEID (Feb. 13, 2012, 1:05 PM), http://www.circleid.com/posts/megabusts_megaquestions_cloud_the_nets_future/, *archived at* http://perma.cc/8494-HU4T.

[202] *See id.* Corwin notes:

> In any event, the number of services from which to choose and their functionality appear to be in at least temporary decline post-MegaBust. The FileSonic and FileServe services disabled all file-sharing within days after, and Upload.to cut off all access from U.S. users (notwithstanding the domain being hosted on the country code TLD of the Pacific Ocean nation of Tonga). Hong Kong-based Filesonic, one of the Internet's top 10 file-sharing sites, terminated its affiliate rewards program. FileJungle and UploadStation disabled all third party downloads, and UploadBox and x7.to shut down all operations.

Id.

[203] *See* Brett Danaher & Michael D. Smith, Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales 24 (Sept 14. 2013) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229349, *archived at* http://perma.cc/QRF8-C2YN.

[204] Corwin, *supra* note 201.

[205] *See* Dotcom Indictment, *supra* note 197, at 42.

[206] *Id.* at 10–11.

[207] Corwin, *supra* note 201.

commentators suggest, for instance, that the same approach could be used against search engines or video-sharing sites for linking to infringing content, or classified-advertisement websites like Backpage or Craigslist that have been criticized for facilitating child exploitation.[208] These latter examples bring us to this Article's final category of technology, designed for legal purposes, but susceptible to illegal use.

C. TECHNOLOGY SUSCEPTIBLE TO ILLEGAL USE: THE TOR PROJECT, SECURITY SOFTWARE

"Onion routing" is a good example of technology clearly created, in the spirit of the hacker ethic, for the betterment of society. In the early 2000s, the U.S. Naval Research Laboratory created software meant to protect online anonymity by passing Internet communications through a network of computers throughout the world.[209] The process works by using layers of relay points, each with its own encryption, to conceal the identity of the originating computer. A long-running project to distribute free versions of this software—now called "Tor," short for "the onion router"—is still largely funded by the U.S. government, through contributions from entities like the State Department and the National Science Foundation.[210] The project is also supported by foreign governments, not-for-profit organizations, and private donors.[211] The Tor project has scores of legitimate uses—law-enforcement officers might use it to disguise a computer's address during an online sting operation, for instance, or persecuted religious groups might rely on it to bypass censorship—but it also lends itself to illegal activity.

The most prominent illegal use of Tor is the Silk Road, an online marketplace, like a black-market eBay, where users can anonymously buy illegal products, primarily drugs.[212] To add to the anonymity, purchases on the Silk Road are made using Bitcoin, a form of online currency stored in a virtual wallet, so that no physical address or person need be tied to it.[213] The

---

[208] *See, e.g.,* Wendi Adelson, *Child Trafficking and the Unavoidable Internet*, 19 SW. J. INT'L L. 281, 289 (2013).

[209] ANDERSON, *supra* note 29, at 232.

[210] *Id.* at 232–33.

[211] *Id.*

[212] *Id.* at 229–30; MIKE POWER, DRUGS UNLIMITED: THE WEB REVOLUTION THAT'S CHANGING HOW THE WORLD GETS HIGH 214–15 (2013).

[213] *See* POWER, *supra* note 212, at 222 ("The architecture of bitcoin, the currency used on the Silk Road by dealers and users, and other services deployed by the site, mean the money *cannot* be simply followed."); *see also* Benjamin Wallace, *The Rise and Fall of Bitcoin*, WIRED MAG., Dec. 2011, at 99.

federal government recently shuttered the Silk Road and captured the site's alleged leader, Ross Ulbricht, known online as "Dread Pirate Roberts," charging him with conspiring to engage in drug trafficking, money laundering, and computer hacking.[214] In two years, the government alleged, the site's users completed roughly 1.2 million transactions generating revenue of nearly 10 million Bitcoin, equating to roughly $1.2 billion (at the time of Ulbricht's arrest).[215]

No court has directly commented on Tor's legality, but it is widely assumed that onion routing, like file-sharing or other anonymizing software, is not illegal of its own accord in the United States.[216] Indeed, even the complaint against Ulbricht, in observing that Tor "is known to be used by cybercriminals," concedes that it "has known legitimate uses."[217] The Electronic Frontier Foundation goes further, explaining that, although it "cannot guarantee" operators of Tor relays "will never face any legal liability," it "believes so strongly that those running Tor relays shouldn't be liable for traffic that passes through the relay that we're running our own middle relay."[218] The Foundation warns, however, that Tor relay operators risk criminal liability "if they monitor, log, or disclose Tor users' communications."[219] Legal commentators generally agree with this

---

[214] Ulbricht was actually charged in two places. The U.S. Attorney in Maryland indicted him by grand jury. Superseding Indictment, United States v. Ulbricht, No. 13-cr-00222-CCB (D. Md. Oct. 1, 2013), ECF No. 4 [hereinafter Ulbricht Maryland Indictment]. And the U.S. Attorney in the Southern District of New York filed a criminal complaint against him. Sealed Complaint, United States v. Ulbricht, 13-cv-06919-JPO, Ex. A (S.D.N.Y. Oct. 2, 2013), ECF No. 4-1 [hereinafter Ulbricht New York Complaint]. Ulbricht was eventually moved to New York, where he went to trial and was found guilty on all seven counts of the New York Complaint. *See* Andy Greenberg, *Silk Road Mastermind Ross Ulbricht Convicted of All 7 Charges*, WIRED (Feb. 4, 2015, 3:57 PM), http://www.wired.com/2015/02/silk-road-ross-ulbricht-verdict, *archived at* http://perma.cc/2XAX-5EXA.

[215] Ulbricht New York Complaint, *supra* note 214, at 15. In June 2014, the United States Marshals Service announced that it would be auctioning off 29,656 Bitcoin seized from Silk Road servers and valued at more than $17.5 million. Cyrus Farivar, *US to Auction 29,656 Bitcoins Seized from Silk Road*, ARS TECHNICA (June 12, 2014, 6:24 PM), http://arstechnica.com/tech-policy/2014/06/us-to-auction-off-29656-bitcoins-seized-from-silk-road-worth-over-17-5m/, *archived at* http://perma.cc/JD8Y-F2MC.

[216] Tor's legality is more questionable in other countries. *See* Keith D. Watson, Note, *The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*, 11 WASH. U. GLOBAL STUD. L. REV. 715, 723–33 (2012) (comparing regulation of Tor in the United States to regulation of Tor in China, Saudi Arabia, and the United Arab Emirates).

[217] Ulbricht New York Complaint, *supra* note 214, at 7.

[218] Electronic Frontier Foundation, *The Legal FAQ for Tor Relay Operators*, THE TOR PROJECT (Apr. 21, 2014), https://www.torproject.org/eff/tor-legal-faq.html.en, *archived at* http://perma.cc/6Z28-9NX2.

[219] *Id.*

assessment: Tor operators who avoid monitoring user communications are shielded from the liability that might arise from illegal transmissions, such as copyright infringement or child pornography.[220] Yet this "shield" sounds a great deal like willful blindness.

Despite this apparent legality, Tor has seemed to some a logical target for regulatory action.[221] Faced with serious threats of cybercrime like illicit drug and firearm sales, and with no easy way to go after suppliers or buyers en masse, the government may view Tor and technologies like it as a vulnerable choke point. If the government can figure out who operates Tor relays, officials may assume they can effectively discourage illegal behavior by narrowing their efforts on these relay operators, viewing them as an easy way to the "blood and flesh" enabling the cloaking of illegal network activity. But targeting Tor relays may lead officials into a wasteful approach where they, as Senator Tom Carper puts it, "play 'whack-a-mole' with the latest website, currency, or other method criminals are using in an effort to evade the law."[222] The Silk Road exemplifies this problem: barely a month after the original site had been shut down, Silk Road 2.0 had emerged, with

---

[220] *See* Watson, *supra* note 216, at 725. Watson noted:

> Because the DMCA was not intended to cover and did not anticipate anonymity networks like Tor, it seems unlikely that a court would apply its provisions to Tor. Furthermore, one might question whether an exit node facilitator could face liability for child pornography charges. There would seem to be liability under 18 U.S.C. § 2252 if someone knowingly facilitated the downloading of child pornography, but the whole point of Tor is that exit-node facilitators do not know what is being routed through their computers.

Id. (citations omitted); Nassim Nazemi, Comment, *DMCA § 512 Safe Harbor for Anonymity Networks amid a Cyber-Democratic Storm: Lessons from the 2009 Iranian Uprising*, 106 NW. U. L. REV. 855, 892 (2012). Nazemi concluded:

> Tor operators, by their very existence, trigger a political dialogue about the importance of online civil liberties, and their services facilitate the development of democratic culture in places like Iran. They demonstrate that Tor has undeniable noninfringing uses that merit protection, and its volunteer operators should thus enjoy full First Amendment protection. At a minimum, they should benefit from § 512(a) safe harbor as conduits of digital communication.

Id. Further, Richard Abbott observes, "Tor's birthplace in the world of intelligence could protect it from any legal attack" because courts may be hesitant to impede the use of a tool that "is truly a national security asset." *See* Richard Abbott, *An Onion a Day Keeps the NSA Away*, J. INTERNET L., May 2010, at 22, 26–27.

[221] *See* Watson, *supra* note 216, at 726 (discussing proposals to regulate Tor).

[222] Press Release, Tom Carper, Senator for Del., Chairman Carper Statement on the Unveiling of the So-Called "Silk Road 2.0" Website (Nov. 6, 2013), http://www.carper.senate.gov/public/index.cfm/pressreleases?ID=8f085bea-7b56-4186-a561-cc37bbf17519, *archived at* http://perma.cc/X5LH-2WR8. *See also* Cyrus Farivar, *Just a Month After Shutdown, Silk Road 2.0 Emerges*, ARS TECHNICA (Nov. 6, 2013, 5:30 PM), http://arstechnica.com/business/2013/11/just-a-month-after-shutdown-silk-road-2-0-emerges/, *archived at* http://perma.cc/7384-DDMP.

drug vendors in tow, and, true to the moniker, a new "Dread Pirate Roberts" at the helm.[223] And when Silk Road 2.0 was eventually shut down, new "Dark Web" services sprouted up, offering even more listings of narcotics for sale than their predecessor.[224] Tor is hardly unique in this respect and may represent a trend: as more and more of the world comes online, the chances of sinking a criminal industry with a single blow decrease as well.[225]

Before predicting how courts might address Tor in a criminal proceeding, consider one more technology that, like Tor, is created for good but highly susceptible to illegal use: network-security toolkits. For as little as $10 per month, any person can pay a "booter" site, like twBooter, for an account allowing the person to launch repeated denial-of-service attacks against a website; a bit more money will buy more accounts, upping the ante of the attack.[226] These attacks can take multiple forms, but the general idea is to overwhelm the target's servers or network connections and disable the site, at least temporarily.[227] The advertised purpose of these services is for sites to test their security—twBooter sells itself as "The Ultimate Administrative Network Stresser Tool"[228]—but the potential for foul play is obvious, especially when the barriers to use are minimal.

---

[223] *Id.* The character of the "Dread Pirate Roberts" comes from the book and the film *The Princess Bride*, which ultimately discloses "that Roberts is not one man, but a series of individuals who periodically pass the name and reputation to a chosen successor." *Dread Pirate Roberts*, WIKIPEDIA, http://en.wikipedia.org/wiki/Dread_Pirate_Roberts (last visited Sept. 22, 2014), *archived at* http://perma.cc/SL3W-8JJK. In fact, that pattern continues: in mid-2014, the second Dread Pirate Roberts stepped down, appointing an interim leader with the pseudonym "Defcon." Ken Klippenstein, *What It's Like to Work for a Darknet Kingpin*, ARS TECHNICA (June 8, 2014, 7:45 PM), http://arstechnica.com/tech-policy/2014/06/punching-the-clock-for-a-darknet-kingpin/, *archived at* http://perma.cc/G92-B4M3.

[224] *See* Greenberg, *supra* note 214 ("Today's leading dark web drug sites like Agora and Evolution offer more narcotics listings than the Silk Road ever did, and have outlived law enforcement's crackdown on their competitors."); Andy Greenberg, *How the Dark Web's New Favorite Drug Market Is Profiting from Silk Road 2's Demise*, WIRED (Nov. 20, 2014, 8:00 AM), http://www.wired.com/2014/11/the-evolution-of-evolution-after-silk-road/.

[225] Richard Abbott makes a similar point in comparing Tor to Napster. Abbott, *supra* note 220, at 26 ("Tor is not Napster. There is no central authority to shut down and no key technology to outlaw. A court order in one country might shutdown a handful of nodes, but the removal of a substantial portion of nodes would require multinational cooperation.").

[226] Sean Gallagher, *Details on the Denial of Service Attack That Targeted Ars Technica*, ARS TECHNICA (Mar. 18, 2013, 4:20 PM), http://arstechnica.com/security/2013/03/details-on-the-denial-of-service-attack-that-targeted-ars-technica/, *archived at* http://perma.cc/RLB7-7NKE (describing "booter" attack on the Ars Technica website).

[227] *Id.*

[228] *See* TWBOOTER[2], http://booter.eu/ (last visited Sept. 22, 2014), *archived at* http://perma.cc/T5RQ-PDX3.

Unauthorized denial-of-service attacks are generally illegal under the Computer Fraud and Abuse Act,[229] but the ultimate question is whether the existence of an obvious illegal use renders the provision of these tools as aiding and abetting.

The answer must be "no," for both network stressors and Tor relays. Like the red dress, these technologies may be used for good or ill, and it is not enough to inculpate a technology provider that it may be better, in terms of income for the business, if illicit activities flourish using the technology.[230] In this sense, the key question is the closeness of operators' relationships with users, not profitability. And that is one of the three key insights for technologists from the substantial unoffending uses analysis.

V. FINAL THOUGHTS ON AVOIDING CRIMINAL LIABILITY

So what are providers of "dual use" technology to do? It will not do to advise them not to "desire" to aid or abet criminal acts with their inventions, nor to implicitly agree to do the same. A clear heart and empty head is a valid defense, but one difficult to prove. Technologists will be tried not for their actual thoughts but for what they appeared to think.

With that in mind, there are three final lessons technologists may take away. First, tailored services carry the greatest risk of criminal prosecution for aiding and abetting. Second, contract provisions will not prevent criminal culpability. Third, employees of technology companies face less risk of liability than their leaders.

A. TAILORED SERVICES CARRY GREATER RISK THAN MASS-MARKET SERVICES

As noted in the discussion of Tor and twBooter, tailored services carry greater risks than do mass-market services. So Tor relays in general have low potential for criminal liability, but Silk Road, which tailors and caters its services to crime, has a much higher liability.

To understand why, analogize Tor relays to transit providers. (The Internet is, after all, the information super-highway.) In *United States v. Heras*, for instance, the defendant knowingly drove a friend to a drug meet, which the Second Circuit found sufficient to support a conviction for aiding

---

[229] 18 U.S.C. § 1030(a)(5)(A)(ii) (2012); *see* United States v. Schuster, 467 F.3d 614, 615 (7th Cir. 2006) (affirming sentence for man convicted under § 1030(a)(5)(A)(ii) for a denial-of-service attack).

[230] *See* Edmund J. Sease, *From Microbes, to Corn Seeds, to Oysters, to Mice: Patentability of New Life Forms*, 38 DRAKE L. REV. 551, 570–71 (1989).

and abetting drug crimes.[231] The friend was otherwise uninvolved in the drug trade but knew that the purpose of the trip was for a drug deal.[232] Changing the relationship with the passenger from friend to customer in a taxicab makes little difference. The taxi driver cannot escape liability by insisting that he only wanted to be paid; many criminal relationships are mercenary. Allowing the taxi driver to escape criminal liability because his motive was payment, not a desire to see the crime succeed, would exonerate the hitman who does not care if his victim dies, so long as he is paid. If the jury believes that the taxi driver knew the trip's purpose, it would not be reversible error to infer a desire to aid the crime.

Critically, the result changes if the defendant drives a bus instead of a taxi. A bus driver who picks up the drug dealer on his normal route, overhears the drug dealer discussing the deal on his cell phone, and drops him off at a regular stop, does not abet a crime. No reasonable jury could infer that the driver had any desire to aid the drug deal, even though he knew the dealer's purpose and also knew that driving his normal route would assist the crime. The bus has a substantial and unoffending purpose even when used by a criminal—the regular, scheduled transport of law-abiding citizens along the same route. Put another way, all of the taxi's bandwidth goes to transporting the criminal, while the bus driver's bandwidth remains available to criminals and citizens alike. Moreover, the bus driver cannot refuse to aid the criminal without interfering with that substantial and unoffending purpose. If the bus driver is made criminal because just one of his riders is a criminal, then criminals would confer liability like a plague to everyone they touched.

Like a virtual bus system, Tor relays provide a means of transmitting information—legal or illegal. Like the bus driver (and unlike the friend or taxi driver), they provide the same service to all, so the knowledge that some users might be criminals does not fairly support an inference of a desire to help them succeed.

The bus driver's defense, however, is not universal. If criminal users may be excluded without interruption of service, and the provider nonetheless permits—and even encourages—illegal uses of the product, as the government alleges with Megaupload, then a jury might fairly infer a desire to encourage criminal acts.[233] Likewise, the defense is inapplicable to mass transit of criminal groups. A jury may justifiably reject a smuggler's

---

[231] 609 F.3d 101, 107 (2d Cir. 2010).

[232] *Id.*

[233] *See* Martin & Newhall, *supra* note 7, at 130–32 (discussing the liability of Megaupload operators).

claim to simply be driving his normal route, mindless of the immigration status of his passengers.

One might think that the encrypted nature of Tor deserves the same inference of guilt, but it does not. Privacy is a substantial and unoffending use for technology. Just as an empty hidden compartment, or a secret cache filled with an embarrassing (but not illegal) collection of Beanie Babies is no crime, so, too, providing the means for secrecy on a mass scale is not aiding and abetting. A lesson for technologists is that tailored services, such as individual tutoring on how to hack a cable modem (or even providing a hacked modem), are far more likely to incur liability than mass-market services, such as writing a book or computer tutorial on how to hack a cable modem.[234] Contact with individual users of a dual technology comes with an inference of a desire to help those users, and if the users are criminals, their criminal aims may be imputed to you.[235]

The importance of noncontact with individual users was on display in the recent acquittal of Raul Rafael Roman Camacho, who found himself charged in a federal indictment because he worked at a business that helped

---

[234] This example comes from the real-life example of Ryan Harris, who wrote the book *Hacking the Cable Modem* (which is exactly what it sounds like) and also ran a website which, among other services, would send users hacked modems. The latter service, the actual hacking of modems, led to Harris's federal conviction when one of his customers turned out to be an FBI agent. *See* Nate Anderson, *How "The Angel" Helped 15,000 People Steal Broadband*, ARS TECHNICA (June 29, 2012, 10:17 AM), http://arstechnica.com/tech-policy/2012/06/how-the-angel-helped-15000-people-steal-broadband, *archived at* http://perma.cc/2ZUC-2LLC; http://perma.cc/PWJ2-94AH. The book, on the other hand, remains available for sale on Amazon.com. AMAZON, http://www.amazon.com/gp/product/1593271018 (last visited Sept. 14, 2014), *archived at* http://perma.cc/F5XT-LXVX?type=image.

[235] Another example is that of Chad Dixon, who received a sentence of eight months for teaching customers how to "beat" a polygraph or "lie detector." *See* Marisa Taylor, *Man Gets Prison for Teaching How to Cheat on Polygraphs*, SEATTLE TIMES, Sept. 7, 2013, at A2. At the same time, many books remain available on beating a polygraph, and one wonders if Dixon could have been convicted for reading them to his clients, as though to a child at bedtime. *See, e.g.*, CHARLES CLIFTON, DECEPTION DETECTION: WINNING THE POLYGRAPH GAME (1991). Perhaps the starkest example would be to compare the infamous book *Hitman: A Technical Manual for Independent Contractors*, with someone giving one-on-one tutelage to a would-be assassin. *See* REX FERAL, HIT MAN: A TECHNICAL MANUAL FOR INDEPENDENT CONTRACTORS (Bruce Scher ed., 1983). The lessons would be aiding and abetting in an elementary sense, even if the murder were never carried out. The book, on the other hand, is not a crime, though it was used to plan and commit a triple murder. *See* Karl Vick, *Horn Convicted in Murders of Ex-Wife, Son and Nurse*, WASH. POST, May 4, 1996, at A1. The book's publisher destroyed all unsold copies of Hitman after the controversy, but the book has found new life on the Amazon Kindle. *See* AMAZON, http://www.amazon.com/Hit-Man-Technical-Independent-Contractors-ebook/dp/B007WU2NFG/ (last visited Sept. 23, 2014), *archived at* http://perma.cc/T4BG-EATK.

people who did not have social security numbers to register their cars.[236] The government alleged that, because the business helped people without social security numbers, the business owner and all the employees were in a conspiracy to "encourage and induce" illegal immigration—i.e., a conspiracy to aid and abet illegal immigrants.[237] The district court granted Roman Camacho's motion for judgment of acquittal, noting that many people without social security numbers were not illegal aliens, such as those on student visas; in other words, the service had a substantial, unoffending use. And Roman Camacho never had contact with any of the customers, so he could not have known any customer was an illegal alien.[238] On the Internet, services like Roman Camacho's can be largely (or fully) automated, and the provider and client never interact at all. Because knowledge of the principal's criminal purpose is essential to a charge of aiding and abetting, such automated services would be less likely to incur criminal liability for aiding and abetting.

B. USELESSNESS OF CONTRACTUAL PROVISIONS DISCLAIMING ILLEGAL INTENT

Misunderstanding the problem and nature of aiding and abetting liability, some lawyers have offered rubbish in lieu of advice: insert clauses forbidding illegal use, require approval for sublicense or resale of technology, and stay informed about how your products and services are used.[239] Some of these suggestions are beyond bad; following them would actually make the situation worse. The suggestion that providers state in licenses and user agreements that criminal use of their technology is prohibited is a fig leaf. No jury would be swayed by such boilerplate disavowals if the criminal use of a technologist's products or services appears obvious in hindsight. Worse, the attempt to paper over the problem is transparent: no customer could claim breach when it was revealed that the customer intended to use the contracted-for products or services to commit a crime. A canny prosecutor would argue that such a clause could serve no other purpose but as an alibi for someone who *wanted* to contract with those with criminal designs. And the advice to "monitor" the customers' use of technology, or even requiring clients to get permission before they resell or

---

[236] *See* United States v. Raul Rafael Roman Camacho, No. 3:12-cr-00067-JD-CAN-3 (N.D. Ind. July 11, 2013) (order granting Rule 29 motion for acquittal on all charges).

[237] *See id.* (quoting 8 U.S.C. § 1324(a)(1)(A)(iv) (internal quotation marks omitted)).

[238] *See id.*

[239] *See, e.g.*, Andrew H. Grant et al., *Software Developer Accused of Aiding and Abetting Illegal Gambling*, PERKINS COIE (Jan. 24, 2013), http://www.perkinscoie.com/files/upload/Update_13_12_Gambling.pdf, *archived at* http://perma.cc/P8US-S5G5.

relicense the technology, rings discordant with both business reality and legal consequence. Knowledge of illegal use has been the lynchpin of successful prosecutions;[240] now counsel suggests actively acquiring such knowledge. That advice goes beyond a warning against reliance on willful blindness; it suggests that clients should deputize themselves as government investigators. Absent an affirmative duty to police their technology, as with contractors selling advanced weapons systems,[241] few companies would willingly adopt such a role. For a few, this will be because the pecuniary benefits of sweeping in illicit customers with innocent ones prove too tempting a lure. But no doubt the overwhelming majority will find policing their customers both impractical and undesirable—even law-abiding customers will object to a perpetual set of eyes reading over their shoulder.

The harsh truth is that lawyers have no easy answers, and purveyors of dual-use technology must accept the risk of prosecution as a cost of doing business and that the likelihood of prosecution (and of conviction) is inversely related to the degree of substantial unoffending uses. The closest thing to a "safe harbor" may be found by analogy to the law of civil asset forfeiture. A car may be forfeited when used in a crime, even if the owner is never charged. But rental car companies do not respond to this by inserting disclaimers in rental contracts against use of the car to transport methamphetamine, nor do they track their customer's movements in an effort to detect smugglers. The company's defense will be to prove one of two things: that they had no knowledge of the crime or that they tried to stop it. The best preparation against a criminal prosecution would be to prepare to meet this higher standard, rather than relying on the lower bar of reasonable doubt. As much as technologists may want to remain neutral, once they have knowledge that a specific user is employing their technology illegally, the only sure way to prevent prosecution is to take some action to stop it, such as cutting off access or even notifying law enforcement.

Unfortunately, however, for those innovators for whom actively assisting law enforcement or interfering with the private decisions of their uses would be anathema, there is only uncertainty. A defense of lack of desire to aid criminal activity will rely on circumstantial evidence; the only direct evidence would be their own statements of their desire, which a jury might dismiss as self-serving. Aware that they will be judged for lack of

---

[240] *See* Watson, *supra* note 216, at 725 ("There would seem to be liability under 18 U.S.C. § 2252 if someone knowingly facilitated the downloading of child pornography, but the whole point of Tor is that exit-node facilitators do not know what is being routed through their computers.").

[241] *See* 22 U.S.C. § 2778 (2012); 22 C.F.R. § 120.1–127.3.

foresight by juries with the benefit of hindsight, dual-use technologists must build a record day-by-day of their own innocence, tailoring their product to discourage illegal uses when possible and justifying every change by reference to its legal uses and markets. Yet this advice is no theriac to criminal liability, only a warning of dangers ahead.

Another option, one increasingly adopted by technologists (and largely untested), has been to craft services and products that can be delivered anonymously, thus preventing the provider from having any knowledge of how the products will be used. Because knowledge can be shown extrinsically, it should be no surprise that the cases reviewing challenges to sufficiency of the evidence to infer intent or desire have seized upon proof of the abettor's knowledge of the principal's intent to commit a crime as sufficient evidence of the abettor's intent do so as well.[242] The existence of substantial, unoffending uses provides some positive, though circumstantial, proof of a *lack* of knowledge. Creating a product such as twBooter that can be used both by those trying to *prevent* hackers and by hackers themselves does not support an inference of a desire to support hackers. And desire to support criminal activity, despite some disagreement, is the mental state courts most consistently require to support a conviction for aiding and abetting.

C. THE POTENTIAL FOR LENIENCY FOR EMPLOYEES

One more minor point. This Article has already discussed how, even though the "substantial unoffending use" approach more consistently resolves the various appellate decisions describing the mental culpability required for aiding and abetting, there remain some gaps to be filled by other inquiries. One of these inquiries is the status of the defendant as an employee.

For example, consider the manufacturing of methamphetamine, which requires large amounts of ingredients commonly found in over-the-counter cold medicine. Certainly cold medicines have substantial, unoffending uses

---

[242] For some recent examples, see, e.g., United States v. Willett, 751 F.3d 335, 340–43 (5th Cir. 2014) (sustaining conviction for aiding and abetting health-care fraud based on evidence defendant knew about upcoding at medical practice); United States v. Lyons, 740 F.3d 702, 715 (1st Cir. 2014) (finding it sufficient to sustain conviction of employee of bookmaking business that he knew the business received bets and he helped it continue receiving them); United States v. Moreland, 703 F.3d 976, 984 (7th Cir. 2012) (explaining that evidence that a seller knew of a buyer's intent to commit a crime with the seller's goods is enough to sustain a conviction for aiding and abetting, though not conspiracy); United States v. Heras, 609 F.3d 101, 107 (2d Cir. 2010) (sustaining conviction for aiding and abetting drug crimes for driver of car who knew his rider's purpose was to deal drugs).

(i.e., the treatment of colds), so the manufacture and sale of cold medicine could not be aiding and abetting in general. But imagine someone is approached outside a drug store by a stranger who asks the person to buy cold medicine and offers reimbursement at five times the retail price.

If the person knew nothing of meth manufacture, and bought the cold medicine suspecting that something illegal *might* be happening but assumed it was something minor, and a jury believed that account, then the person would be acquitted. But a jury might reasonably disbelieve that defense after the prosecution introduced evidence that the person had recently streamed the entire series of *Breaking Bad* online. Under the circumstances, such a high mark-up for cold medicine could impute but one, illicit purpose. Even if the mark-up were much lower, the service provided (buying something on behalf of someone else) has no substantive, legal purpose, which is to say, the stranger could have no legitimate reason to ask someone else to buy cold medicine on her behalf.

But the result might be different if the person was the cashier, and the "substantial unoffending uses" approach does not explain why. A cashier who saw the same people regularly purchasing cold medicine, without symptoms, might suspect (or even know) that the customers were buying it to produce meth. But the instinct is that the cashier, like the bus driver, is not guilty of aiding and abetting. The difference is neither the nature of the product nor the knowledge of how it will be used; it is the evidence that the only desire is not to help the customer but to serve the employer. The cashier and the bus driver are simply doing their job; in that sense, though, their motives are pecuniary, which would not acquit a mercenary, such as a driver who agrees to smuggle people across a border, not out of a desire to help immigrants reach a better life, but out of a desire for the cash paid up front. But it matters that the master served is not a criminal, but a legitimate employer. Even considering the sale of a gun to someone who vows to use it to kill, it matters whether the sale is one by a principal eager to profit from the sale of his gun, or if the sale is rung up by a teenage cashier whose sole focus is on his next cigarette break. But if employees gain a direct interest in the transaction, as with even a slight sales commission, they have the same pecuniary motive as the principal, and a jury may infer the same desire to aid the crime in exchange for cash.

The lesson for technology providers is that digital entrepreneurs and hired guns face greater risk than employees when working on "dual use" technologies. Employee status is not a safe harbor if it becomes clear that the employees' work furthers a criminal enterprise, but employees are less likely to be held liable for aiding and abetting the customers of an employer

than for aiding and abetting customers of their own businesses, absent some profit-sharing arrangement.

CONCLUSION

When and how to allow proof of thought crimes by circumstantial evidence remains the most enduring and integral problem in criminal law. And the "substantial unoffending uses" test is not Alexander's sword that will cleave away complexity. Only a freely given admission of the defendant's own desire to aid a crime has ever offered that clarity. But in the hard cases, those that require an inference of the defendant's desires, the "substantial unoffending uses" test loosens the knot, inviting judges, juries, prosecutors and defense attorneys to tug at another thread, one that will lead to a narrower and more consistent application of the law of aiding and abetting.