*Harvard Journal of Law & Technology*
Volume 31, Number 1 Fall 2017

# ENCRYPTION, GUNS, AND PAPER SHREDDERS: ANALOGICAL REASONING WITH PHYSICALLY DANGEROUS TECHNOLOGIES

*Lydia Lichlyter**

TABLE OF CONTENTS



## I. INTRODUCTION

There are few policy issues on which everyone agrees, but one idea that approaches unanimous support is this: it is within the role of the government to stop people from causing one another serious physical harm and to punish individuals who have caused serious physical harm to others.[1] This idea is foundational to the state's defense and law enforcement activities and is a factor to some degree in several other are-

* Harvard Law School, J.D. Candidate, 2018. I would like to thank Professor Jonathan Zittrain for teaching the fascinating class that led to this Note and for his helpful advice during the editing process, and the staff of the Harvard Journal of Law and Technology, particularly Article Editor Alex Noonan and Editor-in-Chief Daniel Etcovitch, for being wonderful to work with on this and every issue.

1. *Cf.* JOHN STUART MILL, ON LIBERTY 80 (David Bromwich & George Kateb eds., Yale Univ. Press 2003) (1859) ("[T]he only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others."); *see also* Jorge Menezes Oliveira, Harm and Offence in Mill's Conception of Liberty 3 (unpublished manuscript), *available at* http://www.trinitinture.com/documents/oliveira.pdf [https://perma.cc/MK9B-63WX].

as — environmental regulation,[2] food and drug standards,[3] and products liability,[4] for example.

Regulation not of a physically harmful action but of a technology that is used to cause it, however, is more controversial. Virtually no one will argue with a law that makes it a crime to stab someone,[5] but banning all knives would not be an acceptable solution to the American public. And as tragic and common as car accidents are,[6] some people are very uncomfortable with the idea of mandating a complete switch to self-driving cars[7] (which early evidence suggests will be much safer than human drivers).[8] When a new technology is introduced that threatens to cause or contribute to physical harm in some way, calls for its regulation generally follow close behind, and that threat of physical harm often amplifies the emotional rhetoric of the conversation to a fever pitch.[9]

Because new technologies are often difficult to understand and their effects and uses are hard to predict, one technique that individuals may use to argue for a particular regulatory scheme is to say "[New Technology A] is like [Old Technology B], so we should regulate [New Technology A] like we regulate [Old Technology B]." Passwords are like keys or safe combinations[10] and DNA samples are like fingerprints.[11]

---

2. *See, e.g.*, 42 U.S.C. §§ 4391–93 (2012) (authorizing presidential study of public health effects of pollution).

3. *See, e.g.*, 21 U.S.C. § 393 (2012) (creating the Food and Drug Administration with a primary mission to "protect the public health").

4. *See, e.g.*, 15 U.S.C. § 2064 (2012) (requiring manufacturers to notify the Consumer Product Safety Commission if they are aware of a product defect that "creates a substantial risk of injury to the public").

5. The application of that law may, of course, be quite controversial, such as in cases of self-defense.

6. In 2015, there were 35,092 people killed in motor vehicle crashes, and 2,443,000 injured. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., QUICK FACTS 2015 (2016), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812348 [https://perma.cc/99B9-AM3C].

7. *See* James Lileks, *The Next Big Thing the Left Wants to Ban: Human Drivers*, NAT'L REV. (Oct. 7, 2015, 4:00 AM), http://www.nationalreview.com/article/425221/next-big-thing-left-wants-ban-human-drivers-james-lileks [https://perma.cc/W94A-YP2D].

8. *See* Adrienne Lafrance, *Self-Driving Cars Could Save 300,000 Lives Per Decade in America*, THE ATLANTIC (Sept. 29, 2015), https://www.theatlantic.com/technology/archive/2015/09/self-driving-cars-could-save-300000-lives-per-decade-in-america/407956/ [https://perma.cc/Y7PF-2AWA].

9. *See, e.g.*, Cory Bennett, *Homeland Security Chairman: "Biggest Threat Today" Is Terrorists Using Encryption*, THE HILL (Nov. 22, 2015, 11:39 AM), http://thehill.com/homenews/news/261048-house-intel-chair-biggest-threat-today-is-terrorists-using-encryption [https://perma.cc/7GUX-7JA3]; Harriet Taylor, *How the "Internet of Things" Could Be Fatal*, CNBC (Mar. 4, 2016, 12:09 PM), https://www.cnbc.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html [https://perma.cc/WTH9-DCW8].

10. *See* Erin McLaughlin, *Can a Court Make You Give Up Your Password?*, ABC NEWS (Jan. 5, 2012), http://abcnews.go.com/blogs/technology/2012/01/can-a-court-make-you-give-up-your-password/ [https://perma.cc/77RT-XTTP] ("Is a password more like a key to a lockbox . . . or a combination to a safe . . . ?").

And recently, some have argued that encryption is like either guns or paper shredders, depending on whom you ask.[12]

This type of analogical reasoning is completely reasonable and appropriate, particularly in a legal system that relies so heavily on precedent. However, it is not always obvious whether a particular analogy is helpful, or which of two options is more so. Is a taser like a gun, or is it like pepper spray? Is a power saw like a hand saw, or like a power drill? Not every existing physically dangerous technology is regulated the same way, so it would be overly simplistic to simply say that two technologies should be regulated identically because they are both dangerous.

This Note argues that when regulating a new technology that can cause or contribute to physical harm, there are two primary vectors on which two technologies should match for an analogy between them to be helpful in shaping regulation.[13] First, the dangers that the two technologies pose should be of the same kind. Part II describes three categories of dangers, divided by directness. Second, the benefits offered by non-harmful uses of the technology should be of the same kind. Part III describes three categories of benefits. The more similar the two technologies are in these regards, the more useful the analogy will be. Part IV identifies some examples and general implications of these two sets of categories, and Part V discusses how this rubric should be applied to encryption.

## II. TAXONOMY OF DANGERS

There are three categories of ways in which a technology can be used to cause physical harm, and therefore, three kinds of dangers which regulation might address: it can cause harm directly, cause harm within the same course of conduct, or cause harm via a separate action. Generally, the more direct the threatened harm, the more aggressive regulations have historically been, and the more aggressive analogical reasoning suggests they should be in the future.

---

11. *See* Haskell v. Harris, 669 F.3d 1049, 1060 (9th Cir. 2012) ("Given the certain constitutionality of fingerprinting and the clear analogy between fingerprinting and DNA identification under the DNA Act, as amended, privacy concerns here are diminished substantially.").

12. *See* Rob Price, *The FBI Claims Technology Promoted by Apple and WhatsApp Is Helping ISIS*, BUS. INSIDER (June 4, 2015, 7:34 AM), http://www.businessinsider.com/fbi-encryption-going-dark-isis-apple-facebook-whatsapp-steinbach-lieu-2015-6 [https://perma.cc/5DXM-7U7V]. The same analogies to guns (by Benjamin Wittes, Senior Fellow in Governance Studies at the Brookings Institution) and paper shredders (by Professor Jonathan Zittrain, George Bemis Professor of International Law at Harvard Law School), were made at the New England Cybercrime Conference on December 4, 2015, which served as the inspiration for this Note.

13. This Note specifically concerns technologies that can cause physical harm in some direct way. All references to "technologies" or "dangerous technologies" should be interpreted accordingly.

Because the scope of this Note is limited to technologies that pose risks of physical harm, it is also limited to regulations intended to lessen or eliminate those risks. But if the goal of regulating a new technology is to decrease a danger, it is unreasonable to expect an existing regulatory scheme to provide any guidance unless it was designed to address a danger of a similar kind.

### *A. Direct Harms (Category 1)*

The harms in Category 1 are those that most easily come to mind when one thinks of dangerous technologies — uses of a technology that, intentionally or not, directly inflict physical harm. The most obvious examples are weapons, including those intended for nonlethal uses — tasers, pepper spray, police batons, etc. Technologies not intended for use as weapons, but which can cause physical harm if not used properly, like cars and other vehicles, also might be considered within Category 1. Of course, virtually any physical object can inflict Category 1 harms if, for example, it is swung with sufficient velocity;[14] however, those harms are usually not common enough to be a target of regulation. The question is not simply what kinds of harm a technology is capable of causing, but what harms are likely enough to give rise to the question of regulation.[15]

### *B. Harms Within a Single Course of Conduct (Category 2)*

In Category 2 are harms that are caused not directly by a technology but through a course of conduct that includes its use. Here, "course of conduct" is used in the same sense as it often is in the criminal context: a series of two or more actions with a common purpose.[16] Within this category would be the use of technology to destroy evidence of a harmful act, to surveil or track the target of an intended crime, or to communicate with co-conspirators. The common purpose of the course of conduct need not be the harm that results; for example, using technology to facilitate a robbery during which someone was accidentally harmed would be a Category 2 harm as well.

---

14. *But see Lethal Playing Card*, DISCOVERY CHANNEL: MYTHBUSTERS (Apr. 11, 2012), http://www.discovery.com/tv-shows/mythbusters/mythbusters-database/lethal-playing-card/ [https://perma.cc/W29R-RKDP] (debunking the myth that a playing card could be used to kill someone).

15. It may sometimes be that an unlikely harm is alarming enough to motivate policymakers to consider regulation. Though the likelihood of a particular type of harm occurring is not a part of the analogical thinking discussed here, it is of course a relevant factor in crafting a regulatory scheme.

16. *See* WASH. REV. CODE § 10.14.020 (2011).

### *C. Harms via Separate Action (Category 3)*

Finally, Category 3 includes harm that results from an entirely separate action that is somehow enabled or facilitated by the use of a technology. Using a technology to create a weapon, for example, or creating and offering an online service that is later used in a harmful course of conduct, would be actions with Category 3 harms. The outer boundaries of Category 3 are difficult to delineate, since it can be difficult to say at the margins whether the technology's uses here are really causally linked to the harms in any meaningful way.[17] This is likely a significant reason that, historically, actions with only Category 3 harms have tended to be regulated less often and less aggressively, if at all.[18]

## III. TAXONOMY OF BENEFITS

The rationale for requiring a match between harms for a valid analogy is that the two technologies should share a motivation for regulation. When it comes to benefits, the reasoning is the mirror image: the two technologies should also share a motivation for avoiding overregulation. For any dangerous technology, the reason not to simply ban it outright is that it has benefits of some kind, when used in non-harmful ways.[19] Ideally, regulations should be designed to preserve those benefits as much as possible while curtailing the technology's dangers. The type of benefit provided also impacts the way in which users are likely to react to a proposal to regulate the technology; regulations that implicate more important benefits are more likely to be controversial than those that threaten tangential benefits. If an analogy between two technologies is to be useful, the technologies therefore must offer benefits of roughly the same kind.

The three categories of benefits that a dangerous technology may offer are: facilitation of the exercise of a constitutional right, protection of

---

17. A similar issue is frequently encountered in the context of proving proximate causation in negligence cases. *See, e.g.*, Palsgraf v. Long Island R.R. Co., 162 N.E. 99 (1928).

18. *See, e.g.*, Camden R. Webb, *The Crimes of Others: Adam Lanza, Sandy Hook, and Protection Against Tort Liability for Selling Firearms*, LEXISNEXIS LEGAL NEWSROOM (Feb. 4, 2015, 10:10 AM), https://www.lexisnexis.com/legalnewsroom/public-policy/b/public-policy-law-blog/archive/2015/02/04/the-crimes-of-others-adam-lanza-sandy-hook-and-protection-against-tort-liability-for-selling-firearms.aspx?Redirected=true [https://perma.cc/T7Y4-VMST] (discussing the causation principles underlying statutory protection of gun manufacturers); Timothy Dylan Reeves, *Tort Liability for Manufacturers of Violent Video Games: A Situational Discussion of the Causation Calamity*, 60 ALA. L. REV. 519, 536–43 (2009) (describing difficulties of establishing causation of a violent act by a violent video game).

19. For example, calls to ban alternating current electricity over safety concerns in the 1880s and 1890s eventually failed, largely due to alternating current's ability to provide much more efficient delivery, compared to direct current. *See* Matthew Wills, *Thomas Edison and the War of the Currents*, JSTOR DAILY (Sept. 6, 2016), https://daily.jstor.org/thomas-edison-war-currents/ [https://perma.cc/6ZJF-9VDG].

physical health and safety, and economic and convenience benefits. The third category also includes the benefit of allowing users to exercise their preference to use a technology, even in the absence of other objective benefits. To distinguish them from the harms categorized above, these benefit categories are denoted with letters.

### *A. Constitutional Rights (Category A)*

The first benefit that a dangerous technology can provide is the facilitation of users' exercise of a constitutional or other basic right. To be clear, Category A does not include every technology that can be used to exercise a right, but only those that are used to enable those rights in a significant way. For example, a megaphone probably would not fall into Category A, though it could be used in the exercise of the right to free speech, because it generally does not enable speech that would not be otherwise possible. In contrast, social media platforms would be in Category A, since, as the Supreme Court has recognized, they enable users to speak in a fundamentally different way, and users' rights would be significantly curtailed if the platform were unavailable.[20]

Arguably, Category A could include technologies meant to protect users' privacy, but since a general right to privacy has not been clearly defined by the Supreme Court,[21] it is difficult to say that any constitutional right would be impaired if a particular privacy-protective technology were banned. For the time being, it is therefore appropriate to exclude such technologies from Category A.

### *B. Physical Health and Safety (Category B)*

In Category B are technologies that provide benefits to users' physical health or safety, either directly or indirectly. This would include products intended for health purposes, such as pharmaceuticals and medical devices, as well as those used for self-defense, including at least some weapons and security systems.

A difficulty can arise in this category if a technology's users believe it to provide benefits that objectively are not present.[22] Policymakers

---

20. *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017) ("While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace . . . , and social media in particular." (citation omitted)).

21. *See* Katz v. United States, 389 U.S. 347, 350 (1967) ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'").

22. *See, e.g.*, AUSTL. NAT'L HEALTH & MED. RES. COUNCIL, NHMRC INFORMATION PAPER: EVIDENCE ON THE EFFECTIVENESS OF HOMEOPATHY FOR TREATING HEALTH CONDITIONS (2015), https://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/cam02a_information_paper.pdf [https://perma.cc/3JUK-GTTF] (study of 1,800 studies concluding homeopathic treatments have no medical value); David Hemenway & Sara J.

then need to take into account the fact that there will be different perspectives on the value of the technology, and on the benefits endangered by its regulation. If users believe that they are being deprived of a technology that can improve their health, protect them, or save their lives, they are likely to react more emphatically to any proposal that would limit its availability.[23] Depending on the circumstances, it may be helpful to look at both Category B and Category C technologies for analogies in such a case.

### *C. Economic, Convenience, and Preference Benefits (Category C)*

In the final category are technologies that save their users money or time, or which the users simply prefer to use. Though these products are, in a sense, less important than those in Categories A and B, that is not to say that they should be banned or regulated without reason. A government that unnecessarily restricts even frivolous technologies may not be hurting anyone, precisely, but it is certainly not governing well, not to mention wasting its time and resources. However, technologies in this category have historically often been regulated quite aggressively, particularly when they pose serious dangers.[24] It is fair to assume that if two technologies have similar risks, but one offers Category A or B benefits and the other Category C benefits, the latter usually will and should be more strictly regulated than the former.

## IV. EXAMPLES AND IMPLICATIONS

These two sets of categories together create a framework meant to encompass all physically dangerous technologies. By locating other technologies in the same danger and benefit categories, policymakers should be able to make useful analogies and anticipate the effects of various regulatory options.

Both sets of categories described will overlap in some cases; a technology may pose both direct and indirect threats, or may both facilitate the exercise of a constitutional right and offer convenience benefits. Any technology, however, should be treated as falling into the highest-order category that it significantly implicates. By way of illustration, the following table provides examples of products with each possible combina-

---

Solnick, *The Epidemiology of Self-Defense Gun Use: Evidence from the National Crime Victimization Surveys 2007–2011*, 79 PREVENTATIVE MED. 22, 22–24 (2015) (concluding that use of a gun in self-defense "is not associated with a significant reduction in the likelihood of being injured during the crime.").

23. *See* Dwight R. Worley, *Self Defense Argument at Center of Gun Debate*, USA TODAY (Feb. 25, 2013, 9:59 AM), https://www.usatoday.com/story/news/nation/2013/02/25/self-defense-gun-debate/1945591/ [https://perma.cc/ZF5X-KARJ].

24. *See* text accompanying *infra* notes 25–26.

tion of danger and benefit categories. Some products that are not "technologies" are provided for the sake of clarity.

Table 1: Examples of Danger-Benefit Category Combinations

| | | **Danger Categories** | | |
|---|---|---|---|---|
| | | **Category 1: direct harms** | **Category 2: single course of conduct** | **Category 3: separate action** |
| **Benefit Categories** | **Category A: constitutional rights** | Firearms | Communications technologies (telephone, radio, email) | Social media platforms<br>Firearm manufacturing technologies |
| | **Category B: physical health and safety** | Tasers<br>Pepper spray<br>Pharmaceuticals<br>Medical devices | Body armor<br>Crowd dispersal tools | Medical marijuana |
| | **Category C: economic and convenience** | Airplanes<br>Automobiles<br>Alcohol | Paper shredders<br>Smartphones<br>Cryptocurrencies | 3-D printing |

The table is by no means exhaustive, but it should be relatively straightforward to situate most dangerous technologies in the framework. The top left and top right cells illustrate one complication: some technologies may, in a sense, span two cells if, for example, regulation is being considered of both the manufacturer and the user. In such a case, the technology itself, like a firearm, poses Category 1 dangers, while the technology used to create it poses Category 3 ones.

As the table also makes clear, simply locating a technology in a particular cell does not provide an automatic regulatory solution. In the bottom left cell are airplanes, automobiles, and alcohol, which have significant differences in the way they are regulated. However, there are common features that are worth noting, and that should provide guidance in the regulation of other technologies determined to be in that cell. For example, all three industries are heavily regulated by one or more

government agencies,[25] and all three have licensing schemes of some sort.[26] Interestingly, those three industries have also, at least recently, not been the source of much controversy; there has been some disagreement about specifics,[27] but few people dispute the general regulatory structures in place.[28]

The table additionally illustrates comparisons that can be made between the regulatory schemes used in each category. With one notable outlier — medical marijuana, as discussed below — the technologies listed tend to be less regulated as one moves to the right, and regulations tend to be less controversial as one moves from top to bottom. This makes sense; it is reasonable for regulators to be more aggressive in addressing more direct harms, and users are likely to be more defensive of more important benefits.

The outlying example of medical marijuana sheds some light on the value of this framework. Though not, strictly speaking, a technology, marijuana has long been strictly regulated out of a belief that it posed direct dangers to health and offered no significant benefits.[29] It therefore was thought to be in the lower left cell, along with alcohol, airplanes, and automobiles. However, in recent years, as more evidence has been gathered that marijuana may in fact offer some health benefits,[30] and as

25. *See generally* FED. AVIATION ADMIN., OVERVIEW — TITLE 14 OF THE CODE OF FEDERAL REGULATIONS (14 CFR), https://www.faa.gov/regulations_policies/handbooks_manuals/aircraft/amt_handbook/media/FAA-8083-30_Ch12.pdf [https://perma.cc/MM36-5CVZ]; NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., QUICK REFERENCE GUIDE (2010 VERSION) TO FEDERAL MOTOR VEHICLE SAFETY STANDARDS AND REGULATIONS (2011), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/fmvss-quickrefguide-hs811439.pdf [https://perma.cc/PW7P-7NFK]; ALCOHOL AND TOBACCO TAX AND TRADE BUREAU, LAWS AND REGULATIONS UNDER THE FEDERAL ALCOHOL ADMINISTRATION ACT (2006), https://www.ttb.gov/pdf/ttbp51008_laws_regs_act052007.pdf [https://perma.cc/2UJV-TALF].

26. *See, e.g.*, *Driver's License Laws*, FINDLAW, http://traffic.findlaw.com/drivers-license-vehicle-info/drivers-license-laws.html [https://perma.cc/U6GC-4P58]; *Become a Pilot*, FED. AVIATION ADMIN., https://www.faa.gov/pilots/become/ [https://perma.cc/9MNT-XQPD]; *Apply for ABC License*, D.C. ALCOHOLIC BEVERAGE REG. ADMIN., https://abra.dc.gov/node/676542 [https://perma.cc/CWD5-RGU7].

27. *See, e.g.*, Brandon Griggs, *Should the U.S. Lower Its Drinking Age?*, CNN (Jan. 4, 2015, 10:15 AM), http://www.cnn.com/2014/07/16/us/legal-drinking-age/index.html [https://perma.cc/87QG-M7CT] (noting that states have considered lowering the drinking age below 21).

28. *But see* Ryan J. Reilly, *Georgia Republican: Nobody Should Need a Driver's License*, TALKING POINTS MEMO (Feb. 2, 2011, 3:50 AM), http://talkingpointsmemo.com/muckraker/georgia-republican-nobody-should-need-a-driver-s-license [https://perma.cc/7NEQ-ZKLR].

29. *See* Controlled Substance Act of 1970, 21 U.S.C. § 812 (2012) (classifying marijuana as a Schedule I drug with "high potential for abuse" and "no currently accepted medical use.").

30. *See* Jennifer Welsh & Kevin Loria, *23 Health Benefits of Marijuana*, BUS. INSIDER (Apr. 20, 2014, 3:03 PM), http://www.businessinsider.com/health-benefits-of-medical-marijuana-2014-4/ [https://perma.cc/J4WG-LYMC].

its dangers have been questioned more,[31] it has been moved upwards and to the right on the table, and calls have intensified for its decriminalization and deregulation.[32]

Other technologies can show similar shifts. For example, as firearms have become more sophisticated and accessible, they have posed a greater risk of direct harms.[33] Certain categories of guns, like assault weapons, have been specifically targeted by regulations at times because those increasing dangers were not seen as being accompanied by commensurate increases in the benefits offered.[34]

Social media is useful as an example of how, when dangers are indirect enough, regulations may be used to protect a technology instead of to restrict it. Section 230 of the Communications Decency Act ("CDA § 230") prevents website operators from being treated as the speakers of statements posted by users of their sites.[35] CDA § 230 was passed to protect website operators, who play an integral part in ensuring citizens have a platform to exercise their right to free speech.[36] Even when dealing with websites that have allegedly contributed to physical harms, courts applying the law have interpreted it to provide strong protection when the website was only involved in a Category 3 harm manner.[37] Recently, there have been attempts to circumvent CDA § 230 to hold social media sites liable for material support of terrorism based on their provision of services to terrorist organizations.[38] Courts have so far not been sympathetic to these arguments, rejecting them based on the tenuous causal link between the website and the physical harm that occurred[39] and/or on Congress's intent to provide broad protection for free

---

31. *See, e.g.*, Dirk W. Lachenmeier & Jürgen Rehm, *Comparative Risk Assessment of Alcohol, Tobacco, Cannabis and Other Illicit Drugs Using the Margin of Exposure Approach*, SCI. REP. (Jan. 30, 2015), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4311234/ [https://perma.cc/GL5E-WN9Q] (concluding that marijuana poses fewer health risks than alcohol, tobacco, and other drugs).

32. *See, e.g.*, Matt Friedman, *Booker Introduces Bill to Legalize Marijuana Nationwide*, POLITICO (Aug. 1, 2017, 10:22 AM), http://www.politico.com/states/new-jersey/story/2017/08/01/booker-seeks-federal-marijuana-legalization-113716 [https://perma.cc/5QGH-5ZLU].

33. *See* Garry Wills, *Spiking the Gun Myth*, N.Y. TIMES (Sep. 10, 2000), http://www.nytimes.com/books/00/09/10/reviews/000910.10willot.html?mcubz=0 [https://perma.cc/8HXZ-JUWQ].

34. *See* Lois Beckett, *The Assault Weapon Myth*, N.Y. TIMES (Sep. 12, 2014), https://www.nytimes.com/2014/09/14/sunday-review/the-assault-weapon-myth.html?mcubz=0 (last visited Dec. 20, 2017) (arguing that public support for the 1994 assault weapons ban was sufficiently high because "[h]andguns were the weapons most likely to kill you, but they were associated by the public with self-defense," whereas the public and legislators believed that "[c]ivilians did not need to own guns designed for use in war zones.").

35. 47 U.S.C. § 230(c)(1) (2012).

36. *See* Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017).

37. *See, e.g.*, Backpage.com, LLC v. McKenna, 881 F. Supp. 2d 1262, 1273 (W.D. Wash. 2012) (enjoining enforcement of a state statute that criminalizes the offense of advertising commercial sexual abuse of a minor because the statute was likely preempted by CDA § 230).

38. *See, e.g.*, Fields v. Twitter, Inc., 217 F. Supp. 3d 1116 (N.D. Cal. 2016).

39. *Id.* at 1126–27.

speech online.[40] In either case, the logic of the framework is present: the protection extended to a dangerous technology should be, and generally is, based on the directness of the dangers it poses and the importance of the benefits it provides.

## V. ENCRYPTION, GUNS, AND PAPER SHREDDERS

The encryption[41] debate has brought these principles to the fore, as advocates both for and against regulation have attempted to compare encryption to different technologies in an effort to offer solutions. Some of those in favor of regulation have pointed out that encryption can be used by criminals and terrorists to hide evidence of dangerous activity, or to conceal plans from law enforcement surveillance.[42] The term "going dark" was coined by this group to describe the danger: that communications previously accessible to government actors become inaccessible when protected by encryption.[43] Some people in this camp have compared encryption to firearms, arguing that, since both can be used by criminals to cause harm, there are lessons, principles, and/or policies that can be imported from firearms and applied to encryption.[44] The fact that encryption was once classified as a munition for the purpose of export controls[45] highlights how seriously the encryption-firearm analogy could be taken. On the other side, encryption's champions point out that there have always been methods of destroying or hid-

40. *Id.* at 1128 (describing the goal of CDA § 230 as "to promote unfettered and unregulated free speech on the Internet").

41. In this section, the term "encryption" should be understood to refer to widely available strong encryption. Though there is not a clear agreed-upon definition of "strong encryption," it generally refers to methods of encryption that are impossible to break in a reasonable amount of time without access to the decryption keys. *See* Arnold G. Reinhold, *Strong Cryptography: The Global Tide of Change*, CATO INST. Sep. 17, 1999, at 2–3, https://object.cato.org/sites/cato.org/files/pubs/pdf/bp51.pdf [https://perma.cc/RFM4-RDU8].

42. *See* Ellen Nakashima, *FBI Chief: Terrorist Group Turning to Encrypted Communications*, WASH. POST (July 8, 2015), https://www.washingtonpost.com/world/national-security/fbi-chief-terror-group-turning-to-encrypted-communications/2015/07/08/89167f74-2579-11e5-aae2-6c4f59b050aa_story.html?utm_term=.609164eb07f2 [https://perma.cc/G9RL-TVPL]; Jeff John Roberts, *Locked Apple Devices Are Piling Up in Police Evidence Rooms*, FORTUNE (Nov. 17, 2016), http://fortune.com/2016/11/17/locked-apple-devices-are-piling-up-in-police-evidence-rooms/ [https://perma.cc/K7KX-2UWG].

43. *See Going Dark*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/operational-technology/going-dark [https://perma.cc/22Q7-EV9K].

44. *See* Jacob Gershman, *FBI Director Likens Apple Encryption Clash to Gun-Control Debate*, WALL ST. J. (Apr. 12, 2016, 6:45 PM), https://blogs.wsj.com/law/2016/04/12/fbi-director-likens-apple-encryption-clash-to-gun-control-debate/?ref=/blogs/law (last visited Dec. 20, 2017) (noting that "[g]overnment regulations used to classify strong encryption technology as a 'munition' under export-control law").

45. *See* Steven Levy, *Cypher Wars*, WIRED (Nov. 1, 1994, 12:00 PM), https://www.wired.com/1994/11/cypher-wars/ [https://perma.cc/64PD-JEY5].

ing information from law enforcement.[46] Encryption is not like a gun, they say, but like a paper shredder, which can also hide evidence of or plans for a crime from the government.[47]

So, under the framework outlined here, is encryption more like a gun or a paper shredder? This Note argues that the answer is a paper shredder, but with a couple of caveats. Firearms threaten Category 1 direct harms and offer Category A benefits (facilitating a constitutional right).[48] Both encryption and paper shredders threaten Category 2 harm: they can be used in the process of committing a harmful act, such as by destroying evidence, but cannot directly harm people.[49] With both encryption and paper shredders, if the technology is used effectively, it is impossible to tell after the fact whether the information that was hidden was innocent or not. Some circumstantial evidence may be provided by the way in which the technology is used; for example, if someone immediately shreds documents or makes an encrypted phone call immediately after speaking with investigators. However, other evidence is usually needed to prove that the action was nefarious.[50]

Encryption and paper shredders both offer Category C benefits: most individuals using them do so to protect their financial data, and/or based on a personal preference for privacy.[51] Importantly, the two technologies are also similar in that it is difficult, if not impossible, to eliminate their dangerous uses without compromising their beneficial ones. If paper shredders were required not to irretrievably destroy information, both criminals and law enforcement could take advantage of that fact.

---

46. *See* Sam Sacks, *Congressman Warns of Encrypted "Dark Spaces"; Another Says: "Ooooh It Sounds Really Scary"*, THE INTERCEPT (June 3, 2015, 7:23 PM), https://theintercept.com/2015/06/03/one-congressman-warns-encrypted-dark-spaces-another-says-ooooh-sounds-really-scary/ [https://perma.cc/97YP-6EME].

47. *Id.* (quoting Representative Ted Lieu as saying "The notion that encryption is . . . different than other forms of destroying and hiding things is simply not true . . . . Forty years ago, you could make the statement that paper shredders are one of the most damaging things to national security because they destroy documents that law enforcement might want to see.").

48. *See supra* Table 1.

49. It is possible to imagine corner cases in which a paper shredder could injure someone, but such cases are not common enough to be of concern. The closest encryption could come to directly causing harm would probably be a ransomware attack against a hospital, where the unavailability of maliciously encrypted data could harm patients. *See* Kim Zetter, *Why Hospitals Are the Perfect Targets for Ransomware*, WIRED (Mar. 30, 2016, 1:31 PM), https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/ [https://perma.cc/9JH6-6YE4]. However, even in that case, it is the patient's medical condition that directly causes the harm, not the bits of the encrypted data. It is therefore appropriate to consider encryption as being associated with Category 2 harms.

50. *See* United States v. Scott, 776 F. Supp. 629, 632 n.7 (D. Mass. 1991) ("Given the wide use of shredders in this country, shredded documents, standing alone, would not be evidence of criminal activity."), *rev'd on other grounds*, 975 F.2d 927 (1st Cir. 1992).

51. *See* Mary Madden & Lee Rainie, *American's Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ [https://perma.cc/7NRH-UE8R] (ranking various privacy concerns for Americans).

And if encryption schemes provide a mechanism for lawful access to encrypted data, there is a risk that it could also be used for unlawful access.[52]

Some would argue that encryption also has Category A benefits, since it protects the privacy of citizens exercising their right to free speech.[53] Though this could be correct under a broad interpretation of the right to privacy, it is not self-evident that the right to free speech would be meaningfully impaired for American citizens today if encryption were not available.[54] Encryption therefore probably falls into the bottom center cell (Category 2 harms / Category C benefits) of Table 1.

This result suggests that an analogy between encryption and paper shredders is more useful for determining the proper level of regulation than one between encryption and firearms. There is, however, one purpose for which an analogy to firearms might be useful. Because at least some people see encryption as providing Category A benefits, the example of guns could provide some limited guidance for the level of controversy that should be expected in reaction to attempts to regulate encryption.

The question remains: once a valid analogy has been found, how should it be used? It is almost a complete argument to say that encryption is like a paper shredder, and therefore that encryption should be regulated like paper shredders are regulated. However, using this logic ignores a vital link in the argument. Namely, one must also assert that paper shredders (or whatever historical technology is being analogized to) are regulated correctly. The more controversial, evolving, and/or inconsistent the older technology's regulatory scheme is at the present time, the less useful it will be to analogize to it, since it will be unclear at best what the result of the analogy should be. For example, if the analogy between encryption and firearms was a more reasonable one, it is unclear what gun law would provide an appropriate model: a registration

52. *See* Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, SCHNEIER ON SECURITY (July 7, 2015), https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf [perma.cc/FL46-PHNA].

53. *See* Amul Kalia, *Your Right to Use Encryption*, FOUND. ECON. EDUC. (Dec. 27, 2016), https://fee.org/articles/your-right-to-use-encryption/ [https://perma.cc/5PRC-2NDJ]; *see also* Katz v. United States, 389 U.S. 347, 350 (1967).

54. *But see Encryption Key to Free Speech, Says UN Report*, BBC NEWS (May 29, 2015), http://www.bbc.com/news/technology-32916002 [https://perma.cc/2N2W-UHVT].

scheme,[55] a prohibition on access by certain individuals,[56] or a ban on certain more dangerous types of the technology.[57]

This is exactly what makes the analogy between encryption and paper shredders potentially powerful. It would be a hard sell by any encryption regulation advocate, if the validity of the analogy is admitted, to argue that paper shredders are incorrectly regulated, and that analogous regulations to those proposed for encryption should be imposed on shredders. For example, some have argued that it should be illegal to build unbreakable encryption,[58] but it seems absurd to argue that it should be illegal to build shredders that make it impossible to reconstruct shredded documents. If encryption should be regulated more aggressively than a paper shredder, it must be for one of two reasons: either analogical reasoning is completely inappropriate in this case, or the framework presented in this Note is incomplete.

Sometimes a new technology is simply so groundbreaking that analogizing it to existing technologies makes no sense — this may have been the case with the telegram, telephone, printing press, or Internet, for example, which completely revolutionized people's ability to communicate — though it is not clear that encryption has created such dramatic change. It may also be the case that there are overriding concerns other than physical harms at issue; encryption's role in ransomware and cyberbullying, for example, might be paramount. Either argument could be fair, but it is equally fair to suggest that perhaps the fear surrounding the consequences of widespread strong encryption is due more to the technology's quickly growing popularity than to any uniquely difficult danger it creates.[59]

---

55. *See* Firearms Control Regulations Act of 1975, D.C. CODE 1978 Supp. §§ 6-1811–6-1821.

56. *See* David M. Herszenhorn, *Bipartisan Senate Group Proposes "No Fly, No Buy" Gun Measure*, N.Y. TIMES (June 21, 2016), https://www.nytimes.com/2016/06/22/us/politics/senate-gun-control-no-fly-list-terrorism.html (last visited Dec. 20, 2017).

57. *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 110103 (expired 2004) (codifying an assault weapons ban).

58. *See* Joel Hruska, *New York Bill Would Ban Strong Encryption, Mandate Backdoors in All Devices*, EXTREMETECH (Jan. 14, 2016, 8:29 AM), https://www.extremetech.com/mobile/221230-new-york-bill-would-ban-strong-encryption-mandate-backdoors-in-all-devices [https://perma.cc/N6FF-LD5J].

59. *See* Mike McConnell, Michael Chertoff & William Lynn, *Why the Fear of Ubiquitous Data Encryption is Overblown*, WASH. POST (July 28, 2015), https://www.washingtonpost.com/opinions/the-need-forubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html [https://perma.cc/7YB2-TVKM]; BERKMAN CTR. FOR INTERNET & SOC'Y, HARV. U., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE, 1–2 (2016), https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf [https://perma.cc/GHF4-FEMY].

## VI. CONCLUSION

In law, arguments are often won and lost on the strength of their analogies.[60] When it comes to physically dangerous technologies, an analogy's strength is a function of the degree to which two technologies match on the kind of dangers they pose and the benefits they provide. The former has a huge influence on the level of regulation that will be appropriate, while the latter affects how the public will respond to regulation. There are also crossover effects between the categories; regulating technologies with more direct harms is likely to be less controversial, and it is appropriate to protect more important benefits regardless of controversy. It is therefore important that two technologies match on both of these vectors if they are to be compared.

60. *See generally* Jacob M. Carpenter, *Persuading with Precedent: Understanding and Improving Analogies in Legal Argument*, 44 CAP. U. L. REV. 461 (2016).