Assessing Digital Preemption (and the Future of Law Enforcement?)

Daniel Rosenthal*

Forthcoming in the New Criminal Law Review, Fall 2011.

Like "child-safe" toys, modern technological tools can be designed to prevent users from harming themselves and others. For instance, vehicle manufacturers are testing cars that would automatically brake when a collision is imminent.[1] And digital programming can target moral as well as physical harms. The iPhone was designed to allow Apple to remove applications from users' devices, a capability the company utilized to excise sexually explicit applications in early 2010.[2]

Government may increasingly take advantage of the manipulability of digital design to make it difficult or impossible to break laws using digital devices.[3] In a 2008 book, Jonathan Zittrain discusses this law enforcement approach, which he calls "preemption."[4] He sharply contrasts digital preemption with traditional law enforcement techniques premised on the punishment of lawbreaking after it occurs.

Preemption is not new. Governments have often tried to prevent unlawful conduct by manipulating elements of people's environment to make that conduct difficult or impossible. But preemption has never been as important as it is today. Modern digital technology is particularly conducive to preemption, and such technology is becoming part of just about

* I thank Jeannie Suk, Jack Goldsmith, and the members of the Harvard Legal Theory Forum, especially Anthony Kammer. I also benefited from many conversations about this topic with friends and family.

[1] Tim Hornyak, Nissan's Robot Cars Mimic Fish to Avoid Crashing, CNET News, Oct. 2, 2009, available at http://news.cnet.com/8301-17938_105-10366477-1.html.

[2] Jenna Wortham, Apple Bans Some Apps for Sex-Tinged Content, N.Y. Times, Februray 22, 2010. In another example, online dating service eHarmony barred gay users until it was sued for discrimination.

[3] Jonathan Zittrain, The Future of the Internet and How to Stop It 108 (2008) [hereinafter "Future"].

[4] Id.

everything—including cars[5] and books[6] and perhaps, someday, people.[7] For example, digital music files can be controlled through "Digital Rights Management" systems, unlike cassettes or records.[8] Furthermore, cyberspace increasingly facilitates conduct that governments or others want to prevent. This includes the distribution of information deemed dangerous or illegal, such as material released by Wikileaks in 2010.[9] Other crimes have arisen in "virtual worlds," including theft or child pornography.[10] Finally, new technology has coincided with a broad "fundamental shift" towards "preventive and proactive approaches" to controlling harmful conduct, best illustrated by anti-terrorism policies.[11] In light of these trends, digital preemption must be confronted not only by those who study law and technology but also by anyone interested in how regulation might look in the future.

This future could be deeply problematic. While many would welcome any strategy that could dramatically reduce crime, Zittrain argues persuasively that digital preemption gives serious cause for concern.[12] For example, preemptive digital design may be prone to mistakenly

[5] See Ben Charney, Ford in Talks to Add Google Features to its Cars, Dow Jones Newswire, Jan. 7, 2010.

[6] See Douglas MacMillian, Amazon CEO: "Millions" of Kindles Sold, BusinessWeek, January 28, 2010, available at http://www.businessweek.com/the_thread/techbeat/archives/2010/01/amazon_ceo_mill.html.

[7] See Mark Ward, Sensors Turns Skin Into Gadget Control Pad, BBC News, March 26, 2010, available at http://news.bbc.co.uk/2/hi/technology/8587486.stm.

[8] See generally Pamela Samuelson, DRM [and, or, vs.] the Law, Comm. ACM, April 2003.

[9] U.S. government and private companies took steps to reduce access to Wikileaks material, including evicting the material from internet servers.See Anahad O'Connor, Amazon Removes Wikileaks from Servers, N.Y. Times, Dec. 2, 2010 ("Under pressure from federal lawmakers, Amazon.com on Wednesday booted WikiLeaks, the whistle-blowing Web site, from its computer servers, three days after the group released a trove of embarrassing State Department cables and documents.")

[10] Such crime include theft , child pornography, and perhaps even sexual assault. Real Trouble in Virtual Worlds, P.C. Pro, March 11, 2008, available at http://www.pcpro.co.uk/features/176889/real-trouble-in-virtual-worlds.

[11] Alan Dershowitz, Preemption: A Knife That Cuts Both Ways 2-3 (2006).

[12] Future, supra note 3, at 110-126.

preclude lawful conduct.[13] Zittrain admits, however, that "our instincts for when we object to such code are not well formed."[14] Despite preliminary attempts to clarify the issues around digital preemption,[15] this uncertainty remains.[16]

This article attempts to fill that gap by connecting digital preemption to existing literature and analyzing its most significant unexplored risks. The article starts by situating digital preemption among related enforcement techniques, drawing lessons through comparison. Next, the article explores two key objections to digital preemption that have not been developed in previous discussions. The "overenforcement" objection is that, by replacing human discretion with a blunt technological instrument, digital preemption may mistakenly interfere with a great deal of lawful conduct. The "stasis" objection is that digital preemption will eliminate avenues of legal change that depend on lawbreaking and traditional law enforcement. This article concludes with policy suggestions.

I. Putting Digital Preemption in Context

Digital preemption is a law enforcement model in which a government or private party programs a digital device (like a cell phone) or application (like an internet browser) to eliminate opportunities to use that device or application to break the law or engage in other conduct deemed undesirable. Digital preemption occurs now, though it is far less pervasive than it might

[13] Zittrain notes that an internet filter sponsored by the U.S. government prevented access to the U.S. embassy's website because the internet address contained the word "ass." Id at 115.

[14] Id. at 104-105.

[15] In addition to Zittrain, Christina M. Mulligan has discussed preemption in a law review article. Christina M. Mulligan, Perfect Enforcement of Law: When to Limit and When to Use Technology, 14 Rich. J.L. & Tech. 12 (2008).

[16] See Dershowitz, supra note 11, at 7 (describing a lack of debate over the possible "mistakes and perils" of preemption); Rohan Sullivan, Australian Government to Introduce Internet Filter, Associated Press, Dec 15, 2009, http://news.aol.com/article/australian-government-to-introduce/817377 (noting controversy over a national internet filtering system in Australia designed to "block obscene and crime-linked Web sites").

be. YouTube employs a form of digital preemption in its copyright policy, making it difficult for users to violate certain copyrights using the site. The site's software automatically removes videos containing material that matches a database of copyrighted content.[17] The site also removes videos when it receives a copyright complaint.[18] In another example, the U.S. government has mandated that libaries employ internet filters to block access to pornography and other illicit material on library computers.[19] For a less familiar form of digital preemption, imagine handguns that would not fire if held by an unregistered user, as determined by a fingerprint scan, or located within a prohibited area, such as a school zone or public building.[20]

As this collection of examples illustrates, digital preemption can take place in digital environments like cyberspace as well as in the "real" world through devices like cars or handguns that incorporate digital programming. Zittrain and Lawrence Lessig focus on the former—in Lessig's terms, "code as law."[21] One straightforward example is YouTube's copyright policy. Yet, as digital technology pervades everything we do, our "real world" behavior may eventually be shaped by digital programming nearly as much as our online behavior. Compare a person surfing the internet with a person driving in a digitally programmed

[17] Electronic Frontier Foundation, A Guide to YouTube Removals, http://www.eff.org/issues/intellectual-property/guide-to-youtube-removals (accessed August 18, 2010) (describing "content ID match removals" as "automated removals that result when YouTube's computers spot a 'match' between your video and content that has been claimed by a copyright owner")

[18] Id. This policy provides YouTube with a so-called "safe habor" from copyright infringement liability under the Digital Millenium Copyright Act of 1998. 17 U.S.C. § 512(c)(1)(C).

[19] Children's Internet Protection Act, Pub. L. No. 106-554, 114 Stat. 2763A-335 (Dec. 21, 2000), codified at various code sections. The Act is discussed in detail in Section II.
A.1 of this article.

[20] See Jill Barton, Implanted Microchip Would Only Allow Police Officers to Fire Their Guns, Associated Press, April 14, 2004, available at http://www.usatoday.com/tech/news/techinnovations/2004-04-14-smart-chips_x.htm.

[21] See generally Lawrence Lessig, Code: Version 2.0 (2006).

car while listening to an audiobook on a Kindle. Both people can be regulated extensively through digital preemption.

Digital preemption resembles a variety of enforcement practices discussed by criminology scholars under the rubric of "situational crime prevention." While this article focuses narrowly on digital preemption, there is much to learn by comparing digital preemption to situational crime prevention and other similar enforcement models. This section examines digital preemption in light of literature on those models. This section will also briefly discuss "libertarian paternalism," as championed by Cass Sunstein and Richard Thaler.

A. Situational Crime Prevention

Criminologists have defined "situational crime prevention" as "the conscious design or manipulation of immediate environments… to make crime more difficult, more risky, and/or less rewarding… to potential offenders."[22] Situational crime prevention takes many forms.[23] Steering wheel locks are a form of situational crime prevention.[24] So too is conspicuous surveillance, as it increases the cost of crime as perceived by the potential criminal.

Of the different techniques of situational crime prevention, "target hardening" has the most in common with digital preemption. Target hardening involves efforts to create structural barriers within places or objects that might be the target of crime. For example, when drivers employ steering locks, they have "hardened" their vehicle against theft.[25] Similarly, digital

[22] Tim Hope & Richard Sparks, For a Sociological Theory of Situations (or How Useful is Pragmatic Criminology?) in Andrew Von Hirsh, David Garland, and Alison Wakefield, Ethical and Social Perspectives on Situational Crime Prevention 175 (2000).

[23] Ronald V. Clarke provides a helpful table of situational crime prevention techniques in his essay in von Hirsh, Garland, and Wakefield, supra note 22, at 100.

[24] Id.

[25] R.V.G. Clarke, Situational Crime Prevention: Successful Case Studies 66 (1992) (citing R.V.G. Clarke & Derek Blaikie Cornish, Crime Control in Britain: A Review of Policy Research 109 (1983)).

preemption creates structural barriers—the virtual equivalents of steering wheel locks—within the technological tools that criminals might use to violate the law.

Most people encounter target hardening every day. Locks on buildings, cars, and safes are target hardening measures, as are more complex security systems often found at government facilities[26] or sports stadiums.[27] Certainly, the relatively weak locks used to secure most buildings might not merit the label of "preemption" since they can be easily breached. But when advanced enough, security systems can be virtually impenetrable.[28] Besides locks and security systems, property owners might design the architecture or layout of their property to prevent harm in other ways. Neal Katyal describes a variety of such techniques, noting, for instance, that FBI headquarters is "built on stilts to minimize damage in the event of a bomb detonation at street level."[29]

Governments have often turned to situational crime prevention in the context of terrorism. Through metal detectors and body scanners, the American Transportation Security Administration tries to make it impossible to enter an airplane with a weapon or other potentially dangerous material.[30] Through the No Fly list, the Federal Bureau of Investigation aims to make

---

[26] See Stephanie Smith, Cong. Research Serv., The Interagency Security Committee and Security Standards for Federal Buildings (describing five levels of security for federal buildings), available at http://www.fas.org/sgp/crs/homesec/RS22121.pdf.

[27] See Andy Gardiner, Colleges Boost Stadium Security with Federal Help, USA Today, September 8, 2006 (describing elevated security at college football stadiums), available at http://www.usatoday.com/sports/college/football/2006-09-07-security_x.htm?POE=SPOISVA

[28] See Lawrence J. Fennelly, Handbook of Loss Prevention and Crime Prevention (1996) (describing "maximum security" systems able to "impede, detect, assess, and neutralize all unauthorized external and internal activity")

[29] Neal Katyal, Architecture as Crime Control, 111 Yale L. J. 1039, 1071 (2002).

[30] See Passenger Screening, Transportation Security Administration, http://www.tsa.gov/what_we_do/screening/security_checkpoints.shtm (last accessed Jan. 24, 2010).

it impossible for some people to enter an airplane at all.[31] The former is a form of target hardening, while the latter is a form of "access control," another category of techniques within situational crime prevention.[32] Both efforts are motivated by the belief that the government should not merely react to acts of terrorism but must instead work proactively, structuring environments to minimize opportunities for attacks.[33]

Finally, governments and others have often used preemptive techniques to preserve vehicle safety. In 1972, the American National Highway Traffic and Safety Administration amended its regulations to allow car manufacturers to comply with safety rules by installing ignition interlock systems in new cars.[34] Such systems would make it impossible to start a car if its seatbelts were not engaged, preempting drivers' ability to drive without wearing their seatbelts.[35] After a federal court struck down the other compliance options in the regulations,[36] ignition interlock systems briefly became mandatory.[37] The interlock regulation provoked significant controversy, and Congress eliminated it in 1974.[38] But ignition interlock systems

[31] Five Years After The Intelligence Reform and Terrorism Prevention Act: Stopping Terrorist Travel: Hearing Before the Senate Committee on Homeland Security and Governmental Affairs (2009) (testimony of Timothy J. Healy, Director, Terrorist Screening Center) (noting that 3400 people, including 170 "U.S. persons" are on the No Fly list.).

[32] Andrew von Hirsch & Clifford Shearing, Exclusion From Public Space, in Von Hirsh, Garland, and Wakefield, supra note 22, at 77.

[33] Dershowitz, supra note 11, at 7 (noting that deterrence requires society to be willing to withstand some level of violations).

[34] See Chrysler Corp. v. Department of Transp., 472 F.2d 659, 666 (6th Cir. 1972).

[35] See id. (describing ignition interlock systems to prevent ignition "unless the driver and any front seat passengers have fastened their seat belts").

[36] Id.

[37] See Jerry L. Mashaw, The Struggle for Auto Safety 133 (1990).

[38] See id. at 134-140 (describing an intense congressional debate weighing the safety benefits of interlock devices against their costs in convenience and "big brotherism").

persist. Today, many states authorize the installation of such systems in the vehicles of people convicted of drunk driving.[39] The systems administer a breathalyzer before the car will start. The U.S. government has backed a campaign to install such systems in all cars.[40]

Digital technology makes situational crime prevention much more feasible. In the vehicle safety context, for example, manufacturers could use digital programming to prevent a wide range of harmful conduct. In new Ford cars, parents can make it impossible for their children to drive faster than a preset maximum speed.[41] It would be easy for the government to impose such limits on *all* drivers through technology. And preemption is already becoming common in cyberspace, the site of a rapidly increasing share of commercial and recreational activity. Recall YouTube's copyright policy and online pornography filters.

B. Libertarian Paternalism

Situational crime prevention is closely related to "libertarian paternalism," as discussed by Cass Sunstein and Richard Thaler in their book, *Nudge*.[42] Indeed, libertarian paternalism can be described as the non-criminal mirror image of situational crime prevention. As described by Sunstein and Thaler, "nudges" reshape people's environment to prevent them from engaging in conduct that is undesirable but not generally illegal.[43] The similarities become clear when

[39] See, e.g., Arizona Revised Statutes § 28-1401 (allowing a person convicted of drunk driving to apply for a "special ignition interlock restricted driver license that allows the person to operate a motor vehicle during the period of suspension or revocation"); Fla. Stat. § 316.193 (requiring the placement of ignition interlock devices in all vehicles owned and routinely operated by a person upon their second conviction for drunk driving).

[40] For more detail on this possibility, see infra Section I.C.1.

[41] Chris Woodyard, Ford to let Parents Censor Teens' Car Radio, USA Today, Dec. 29, 2010.

[42] Richard H. Thaler & Cass R. Sunstein, Nudge (2008).

[43] A further difference is that techniques of situational crime prevention are sometimes more coercive than Sunstein and Thaler would portray "libertarian paternalism" to be.

comparing several examples from *Nudge* with examples from the literature on situational crime prevention.

For example, Sunstein and Thaler note that homeowners could be nudged to conserve energy if thermostats made the price of energy consumption more salient by displaying energy use and costs.[44] Meanwhile, Ronald V. Clarke identifies roadside speedometers as a situational approach to reducing speeding through salience.[45] Sunstein and Thaler praise systems that allow gambling addicts to place themselves on a list of people banned from casinos,[46] a form of "access control" that mirrors the government's terrorist watch list. And just as children could be discouraged from eating unhealthy food by to the layout of a cafeteria,[47] people could be discouraged from drunk driving by the placement of bars close to public transportation, a technique of situational crime prevention.

Similarly, libertarian paternalist techniques have analogs in digital preemption. Digital tools could be programmed to make unlawful behavior more salient, just like Sunstein and Thaler's thermostat or Clarke's speedometer. And users could be barred from accessing websites or applications based on their prior offenses or their own desire to eliminate temptation, just as gambling addicts could be excluded from casinos.

[44] Thaler & Sunstein, supra note 42, at 99. Subsequent research has validated this suggestion. John Tierney, Are We Ready to Track Carbon Footprints, N.Y. Times, March 25, 2008, available at http://www.nytimes.com/2008/03/25/science/25tier.html

[45] Clarke in von Hirsh, Garland, and Wakefield, supra note 22, at 100

[46] Thaler & Sunstein, supra note 42, at 233.

[47] Id. at 1-3.

C. Three lessons for digital preemption

The payoff to these comparisons is that lessons from other bodies of literature can be applied to digital preemption. This section highlights three such lessons, all of which contradict or amend assumptions in previous discussions of digital preemption.

1. Digital preemption is not unprecedented and, like its predecessors, may gain broad public acceptance

Academics have sometimes potrayed digital preemption as an unfamiliar and novel prospect. In discussing this kind of regulation, Lawrence Lessig writes that "[c]yberspace demands a new understanding of how regulation works,"[48] and Zittrain echoes this sentiment.[49] In truth, digital preemption is less of a revolution than an extension of existing regulatory techniques. Governments and powerful private have always been able to affect people's behavior through manipulation of their environment. This is evidenced by numerous examples of situational crime prevention and libertarian paternalism.

People seem comfortable with many of the preemptive techniques discussed in the previous sections. Preemptive approaches to terrorism have gained wide acceptance.[50] Similarly, no one has ever complained that criminals should be free to break into buildings so long as they are willing to face the consequences. Instead, we are happy to let landowners and banks work to preempt intrusions. Many of Sunstein and Thaler's "nudges" are relatively uncontroversial as well.

---

[48] Lessig, supra note 21, at 5.

[49] See Future, supra note 3, at 107-10 (contrasting technological "perfect enforcement" with traditional enforcement methods).

[50] See James Gordon Meek, Poll: Only 20% of Americans Object to Airport Body Scans by Security Screeners, New York Daily News, Jan 12, 2010 (describing public approval of full body scans to prevent passengers from bringing weapons onto airplanes).

Still, people may react differently to digital preemption for two reasons. First, digital preemption may be more restrictive than other preemptive techniques. Compare roadside speedometers to car engines that stall when a driver exceeds the speed limit. Both prevent speeding by restructuring the driver's environment. But the second would likely provoke significantly greater opposition because it seems to deprive the driver of choice altogether.

Second, digital preemption will often target less severe harms other preemptive enforcement techniques, at least in the near term. For example digital preemption probably will not prevent violent crime anytime soon. Instead, as Zittrain's examples illustrate, much digital preemption might focus on enforcing copyright and intellectual property laws.[51] In contrast, many non-digital preemptive techniques, including airport security measures, are targeted at the worst kinds of harms. But it would be a failure of imagination to believe digital preemption will never target significant physical and economic crimes. Consider vehicle safety measures, control of digitized firearms, and efforts to prevent financially ruinous cyberattacks.

Ignition interlock technology provides a sketch of how digital preemption might be accepted by the public over time. As noted earlier, in the 1970s, the federal government briefly required cars to come installed with technology that would prevent the engine from starting unless the driver was ensconced in a seatbelt. But the regulation was quickly scrapped, as interlock systems were seen as inconvenient and intrusive.[52]

Yet, the federal government evidently believes that similar systems to prevent drunk driving may soon be politically feasible. This is likely due in part to the serious harms arising from drunk driving. The government is funding research into such systems, which could be

[51] Future, supra note 3, at 103-104, 108, 109, 111, 119-120.

[52] See Mashaw, supra note 37, at 134-140 (describing an intense congressional debate weighing the safety benefits of interlock devices against their costs in convenience and "big brotherism").

mandated for all cars. The new systems would measure BAC unobstruvisvely and accurately. Perhaps learning from the controversies of the 1970s, the government and its private partners have proceeded carefully. Indeed, the partnership's public statements read as if designed to obscure the fact that either government or industry is involved.[53] But after it tests the water, the government may again propose mandatory ignition interlock systems. If it does so, insurance companies[54] and traffic safety interest groups[55] will likely offer their support, and the proposal might gain popular approval.[56] Similarly, many forms of digital preemption will likely gain eventual public acceptance if they are and targeted at the right sorts of harms and carefully promoted.

2. Digital preemption will not place a total bar on choice or eliminate targeted crime altogether

Preemption seems to place a much more severe burden on choice that traditional law enforcement. Instead of punishing crime after it occurs, preemption aims to make crime impossible.[57] Zittrain writes that digital preemption could make personal choices "vanish."[58]

---

[53] See, e.g., Press Release, Major Advancement for Efforts to Eliminating Drunk Driving: Research Awards Granted to Three Companies, September 25, 2009, available at http://www.dadss.org/. The release does not mention the involvement of NHTSA until the fourth paragraph. Even then, it never states that NHTSA is part of the federal government. Similarly, it does not highlight the involvement of the Automotive Coalition for Traffic Safety or state that the coalition members are car manufacturers and insurance companies.

[54] New Survey Results: Stop Anyone Impaired by Alcohol From Driving Any Vehicle, Public Says, PR Newswire, September 17, 2009 (quoting the vice president of the Insurance Institute for Highway Safety in support of mandatory interlock systems in all vehicles).

[55] See Mothers Against Drunk Driving, Ignition Interlock, http://www.madd.org/Drunk-Driving/Drunk-Driving/Campaign-to-Eliminate-Drunk-Driving/Ignition-Interlocks.aspx (last accessed Jan. 23, 2010) (advocating mandatory interlock systems for all convicted drunk drivers on the first offense).

[56] According to a survey performed by the Insurance Institute for Highway Safety, 64 percent of Americans would support a mandatory ignition interlock law for all cars. Supra note 54.

[57] Some forms of traditional law enforcement also aim to prevent crime by eliminating choice, for example through inchoate liability or injunctions.

[58] Future, supra note 3, at 122.

Proponents and critics of digital preemption both focus on choice. For proponents, the power of preemption as a law enforcement tool stems from its ability to foreclose illegal choices. But critics are disturbed by the prospect that the government could deprive individuals of choice, even in an effort to prevent crime.[59]

The real story is more nuanced. At its most effective, digital preemption would eliminate people's ability to use *certain* tools to carry out *certain* crimes. More commonly, digital preemption would be susceptible to workarounds. Scholars of digital preemption should draw on the literature of situational crime prevention, which acknowledges and often focuses on the limits of preemptive techniques in affecting choice. Criminologists have explained that situational crime prevention makes crime more difficult but not impossible. And they have devoted significant effort to exploring "displacement," the shifting of criminal behavior from crimes or targets that have been preempted to other crimes or targets.

Like other forms of situational crime prevention, digital preemption will usually not eliminate choice altogether and may lead to significant displacement. Consider first that many current forms of digital preemption can be bypassed without great effort or expertise. For example, protections on music files purchased in the iTunes store can be "easily circumvented," according to Zittrain.[60] Zittrain believes that such circumvention will be possible so long as people use "generative" devices that can be freely programmed by users. He notes that such devices allow users to utilize code written by "subversively minded techies" to overcome

---

[59] See Future, supra note 3, at 112 ("Part of what makes us human are the choices that we make every day about what counts as right and wrong, and whether to give in to temptations that we believe to be wrong. In a completely monitored and controlled environment, those choices vanish.").

[60] Jonathan Zittrain, The Generative Internet, 119 Harv. L. Rev. 1974, 2000 (2006).

preemptive restrictions on their behavior.[61] Yet, even in a world of non-generative "tethered appliances,"[62] preemption may often fall short of complete effectiveness. The iPhone, cited by Zittrain as a tethered appliance,[63] can be "unlocked" to bypass its built-in limitations.[64] As technology advances, hacking techniques may advance as well.

Furthermore, even if a tethered appliance were able to preempt conduct with total effectiveness, people could still turn to other tools to commit crime, including non-digital tools. For example, suppose that someone wants to access child pornography on their iPad, but that the tablet is equipped with an impenetrable filter. The person might turn to an old, untethered PC or find a way to purchase printed pictures.

Still, like other forms of situational crime prevention, digital preemption would discourage lawbreaking by increasing the costs and inconvenience of illicit conduct.[65] In this way, preemption would function as a "nudge" against the targeted conduct, not a complete bar.[66] But under the right circumstances, digital preemption would become less like a nudge and more like a headlock. Sophisticated digital preemption might allow choice only to people with

---

[61] Future, supra note 3, at 105-6.

[62] See id. at 101 (describing "tethered appliances" as "centrally controlled… information appliances like mobile phones, video game consoles, TiVos, iPods, iPhones, and BlackBerries").

[63] See id.

[64] Tim Wu, The iPhone Freedom Fighters, Slate, Oct. 4, 2007, available at http://www.slate.com/id/2175304/.

[65] For example, imagine that someone wants to break into a building that has been fortified with very secure locks. A determined thief will use sophisticated or powerful tools to enter the building, steal a key or bribe a security guard. While these methods are available, they require more time and resources than breaking into an unsecured building, and they raise the probability of being caught and punished, another cost. See Katyal, supra note 29, at 1089 ("When target-hardening measures and access controls are employed, only those criminals who have the sophistication and tools to circumvent these defenses will be frequent violators… Some empirical evidence suggests that burglars are sensi-tive to fences and locks; one reason is that such devices increase the cost of committing a criminal act.").

[66] See Sunstein & Thaler, supra note 42, at 8 (Yale University Press, 2008) (defining "nudge" as an "aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives).

sufficient technical knowledge, creativity, or resources to circumvent the system. Additionally, digital preemption may serve to eliminate impulsive lawbreaking, because people would have to devote time to finding ways around the preemptive bar.

However, even when digital preemption completely eliminates one kind of illegal behavior, it may not lead to an equivalent net decrease in crime due to displacement.[67] Criminologists have vigorously debated the significance of displacement.[68] Those interested in implementing digital preemption should consider the issue further.

3. Digital preemption raises a variety of moral and ethical questions, many of which have been explored previously in criminology literature.

Digital preemption raises difficult moral and ethical questions. These questions are mostly outside the scope of this article, which focuses on the practical impacts of digital preemption. But it is appropriate here to comment briefly on these issues and describe how they have been dealt with in the literature on situational crime prevention.

Criminologists have considered whether preemptive enforcement might lead to a society poorer in public morality, openness, or trust,[69] and these concerns seem firmly applicable to digital preemption. One common line of analysis starts by arguing that, by anticipating unlawful behavior, preemptive enforcement sends a message that criminal impulses are expected.[70]

---

[67] See Ian Ayres & Steven D. Levitt, Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack, 113 Quarterly Journal of Economics 43 (1998) (noting that steering wheel locks likely shift crime to different victims).

[68] See Ronald V. Clarke, Situational Crime Prevention in Wortley & Mazerolle, Environmental Criminology and Crime Analysis 187 (2008).

[69] See, e.g., R. A. Duff & S. E. Marshall, Benefits, Burdens, and Responsibilities: Some Ethical Dimensions of Situational Crime Prevention, in von Hirsh, Garland, and Wakefield, supra note 22, at 22.

[70] See John Kleinig, The Burdens of Situational Crime Prevention: An Ethical Commentary, in Von Hirsh, Garland, and Wakefield, supra note 22, at 42 (discussing the view that situational crime preemption relies on the notion that "human weaknesses are widespread" and "nobody is exempt from temptation" (internal quotation marks removed).

Furthermore, by preventing such behavior rather than punishing it, preemptive enforcement sends a message that criminal impulses are undeserving of retribution. Indeed, observers might conclude that people are not really responsible for their attempted—or even completed—illegal acts.[71] Rather, offenders might simply have found themselves in situations that have not been adequately structured to prevent crime. Furthermore, observers might think that victims of crime are themselves partly to blame for creating these situations. From one perspective, this view of crime is exactly right.[72] From another, it is dangerous and morally flawed.

Another concern is that the benefits and burdens of preemption will be distributed unfairly across people and communities.[73] The most troubling version of this concern holds that preemption will disproportionately benefit the wealthy and burden others. For example, gated communities are a form of preemption that favors the subset of population that can afford to live in them. And access control measures are usually targeted at people who fit the stereotypical profile of criminal offenders: young, poor, and often minority.[74] It is unclear how these concerns might translate to the context of digital preemption. Perhaps digital preemption will be more equitable than other preventative enforcement measures because of its broad systematic application. Digital code does not distinguish between rich and poor. Furthermore, digital preemption often burdens technology users, who are disproportionately wealthy. Still, this area should be examined further.

Additional ethical issues may arise from the role of private organizations in implementing digital preemption. For example, in an effort to filter child pornography on the internet, the

[71] Id. at 53 (attributing this view of Felson and Clarke, as well as Harel).

[72] Id.

[73] Duff & Marshall, supra note 69, at 24-27.

[74] Alison Wakefield in Von Hirsh, Garland, and Wakefield, supra note 22, at 131.

government would likely work with Internet Service Providers, companies that create internet browsers, companies that create operating systems, manufacturers of mobile computing devices like smart phones, or some combination of these. Criminologists have analyzed "third party policing" efforts,[75] though they have not focused on the kind of organized regulation of third parties that would likely accompany effective digital preemption. Meanwhile, private organizations may employ digital preemption on their own initiative, just as private parties use locks to prevent property theft. This possibility is discussed briefly in Section III of this paper. The private implementation of digital preemption deserves further exploration.

II. The risks of digital preemption

Zittrain and others have written insightfully about the dangers of digital preemption. Zittrain presents six types of objections to "perfect enforcement," a category that includes digital preemption.[76] Following Zittrain, Christine Mulligan poses nine questions that should be asked to evaluate the use of technology to enforce a law.[77] While these analyses are excellent starting points, they are not the final word. First, Zittrain and Mulligan group digital preemption with other forms of technological enforcement, obscuring the unique issues posed by preemption. Second, both authors paint with a very broad brush, discussing the risks of digital preemption generally without providing much guidance on how to assess these risks in particular situations. Partly as a result of these gaps, readers may be prone to dismiss any proposed application of digital preemption as unjustifiably dangerous, notwithstanding that the authors' views are more

[75] See generally Loraine Mazerolle & Janet Ransley, Third Party Policing (2005).

[76] The categories are: objections to the underlying substantive law, portability and enforceability without the rule of law, amplification and the lock-in of mistakes, bulwarks against the government, the benefits of tolerated uses, and the undesirable collapse of conduct and decision rules. Future, supra note 3, at 111-23.

[77] See generally Mulligan, supra note 15.

nuanced.[78] This section presents a different and, I hope, more useful framework for thinking about the risks of digital preemption. It focuse on the dangers of "overenforcement" and "stasis" that may accompany the use of digital preemption in place of traditional law enforcement techniques.

A. Overenforcement

As noted by Zittrain and others, one substantial risk of digital preemption is that preemptive techniques may apply the law inaccurately.[79] This is particularly likely when the law involves complex or subjective standards, exceptions, or defenses.[80] The key concern here is avoiding overenforcement, the preemption of conduct that is not in fact unlawful.[81]

1. Which laws will be overenforced?

One might doubt that *any* law could be applied accurately by digital code. In fact, some prohibitions might be enforced by a digital algorithm with little risk of overenforcement. Consider a typical drunk driving law, making it illegal for a person to drive when his or her blood alcohol level (BAC) exceeds 0.08. The law is easy to apply. To determine whether a person has violated the law, one needs only to know whether that person has a BAC over 0.08 and whether that person is driving. There are generally no exceptions to the law; drunk driving is always illegal. It is hard to imagine any plausible defense available to someone who has

[78] See, e.g., Future, supra note 3, at 123 (concluding that there is a "balance to be struck rather than an unmitigated good in perfect enforcement").

[79] This corresponds with Zittrain's concern about "Amplification and the Lock-in of Mistakes." Id. at 114. In addition to mistakes, this section touches on Zittrain's discussion of the public interest in free flow of information, as well as the "benefits of tolerated uses."

[80] See, e.g., Mulligan, supra note 15, at 29-31 (arguing that preemptive techniques may be incompatible with the necessity defense).

[81] Although preemption may also underenforce, this would be less troubling. Presumably, traditional law enforcement techniques could target violations that were not preempted.

driven while intoxicated, except in extraordinary circumstances.[82] Furthermore, because drunk driving is highly dangerous,[83] we might tolerate a small risk of overenforcement in order to save many lives. Thus, this law may be a good candidate for preemption.

However, many laws are too complex to apply through an algorithm, at least within current technical capabilities. These laws have complicated exceptions and defenses or involve subjective inquiries. Consider laws targeted at online obscenity. The obscenity doctrine under the First Amendment does not lend itself to enforcement by digital code. [84] Indeed, for many years, the Supreme Court held "movie days"[85] because, as Justice Potter Stewart famously wrote, the only way he could decide whether material was obscene was to "know it when I see it."[86]

This problem is illustrated by the Children's Internet Protection Act (CIPA), passed by Congress in 2000.[87] CIPA limits federal funding to libraries that do not install filtering software to block obscene material on the internet.[88] Critics claimed that filters would significantly "overblock" by barring access to material that was outside the scope of CIPA and protected by

[82] One possibility is that a violator could claim necessity if she were, for example, trying to escape from an eminent assault or driving a friend to the hospital. Even in these situations, the violator would have to show that there were no other alternatives.

[83] According to one estimate, in 2007, "13,470 people died in alcohol-related crashes, accounting for one third (32%) of all traffic-related deaths." Centers for Disease Control, National Drunk Driving and Drugged Driving Prevention Month, available at http://www.cdc.gov/MotorVehicleSafety/Impaired_Driving/3d.html (last accessed Jan. 24, 2010).

[84] The obscenity standard is laid out by Miller v. California, 413 U.S. 15, 23-25 (1973) (holding that the state can regulate material "which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way, and which, taken as a whole, do not have serious literary, artistic, political, or scientific value").

[85] Bob Woodward and Scott Armstrong, The Brethren 238-240 (1st paperback ed., 2005) (1979).

[86] Jacobellis v. Ohio, 378 U.S. 184, 197 (1964).

[87] Pub. L. No. 106-554, 114 Stat. 2763A-335 (Dec. 21, 2000), codified at various code sections.

[88] 20 U.S.C.S. § 9134.

the constitution.[89] Overblocking occurs because filtering software delegates difficult subjective inquiries to digital code. In defending CIPA in court, the government did not contest that filters would overblock.[90]

Though the Supreme Court ultimately upheld CIPA's filtering provision,[91] the Court's opinion highlights the perils of overenforcement due to digital preemption. Filtering was acceptable in part because patrons who encountered "overblocking" could ask the staff to disable the software.[92] Other forms of digital preemption might not include this form of escape. Furthermore, the Court found that library content is traditionally tightly controlled by library staff, making restrictions on library browsing more acceptable.[93] The Court's reasoning suggests that compelled filtering would be unconstitutional in many contexts outside libraries due to the risk of overenforcement.[94]

2. Evaluating overenforcement

[89] Brief of Appellees American Library Association, et. al. at 59, United States v. Am. Library Ass'n (Feb. 10, 2003) ("Internet filtering software is a blunt instrument that blocks far more speech than CIPA requires… [A] large portion is sexually explicit but non-obscene material that is protected at least for adults.").

[90] Brief for Apellants United States at 12, United States v. Am. Library Ass'n (Oct. 29, 2002) (acknowledging that "filtering software erroneously blocks a fraction of 1% of the material on the Internet").

[91] Am. Library Ass'n, 529 U.S. 194. The court squarely took on the question of whether filtering was an unconstitutional restriction on speech. See Am. Library Ass'n, 529 U.S. at 243 ("[W]e must ask whether the condition that Congress requires would be unconstitutional if performed by the library itself." (internal quotation marks, ellipses omitted)).

[92] Am. Library Ass'n, 529 U.S. at 208-9.

[93] See id. at 204 ("Although they seek to provide a wide array of information, their goal has never been to provide universal coverage… libraries collect only those materials deemed to have requisite and appropriate quality." (quotes, citations removed)).

[94] For example, in Ashcroft v. ACLU, 542 U.S. 656 (2004), the Court considered discussed filtering as a less restrictive alternative to the Child Online Protection Act (COPA). COPA aimed to combat obscenity not just in libraries but in any access to the world wide web. The Court wrote that Congress could "take steps to promote [filter] development by industry, and their use by parents,"id. at 669, but neither the majority opinion nor any of the other opinions suggested that Congress could *require* the use of filters outside libraries or other analogous contexts.

The examples above illustrate that overenforcement is more worrisome in some situations than others. To evaluate the risk in a particular situation, two questions should be asked. The first question is how frequently overenforcement would occur. The second question is how harmful overenforcement would be.

The answer to the first question will depend largely on the mechanics of the preemptive technique, but several general principles can help indicate whether a law might be enforced accurately through digital code. Preemption will likely make many mistakes in enforcing laws that require subjective, case-specific inquiries to determine liability, such as obscenity restrictions. Similarly, laws that often provoke the use of affirmative defenses like fair use or self-defense will be poor candidates for preemption. So too will laws that are designed to be enforced only at the discretion of a private party, like many copyright restrictions. For example, copyright restrictions under the Digital Millennium Copyright Act (DMCA) are enforced through a discretionary "notice and takedown" regime.[95] To apply the law, the algorithm would have to check to see if the copyright holder wishes to issue a takedown notice. On the other hand, laws that can be stated as a straightforward rule with few exceptions, like drunk driving laws, might be enforceable through preemption with little overenforcement.[96]

But this analysis is only the first step in assessing overenforcement. Lawmakers should also gauge the acceptability of overenforcement in the particular context at issue. In general, our legal system tolerates very little overenforcement. This is evidenced by the procedural and evidentiary protections for criminal defendants, including the state's high burden of proof in

[95] Future, supra note 3, at 119.

[96] See Henry Hart & Albert Sachs, The Legal Process: Basic Problems in Making and Application of Law (Tenth ed. 1958) (noting the "miracle" of "innumerable legal rules" which "function[] successfully as… rule[s] without the necessity of further elaboration").

criminal proceedings. To use Alan Dershowitz's terminology, much criminal law arises from the belief that "false positives" (wrongful convictions) are much more harmful than "false negatives" (wrongful acquittals).[97] But our tolerance for false positives and false negatives may vary greatly depending on the crime in question and the injury incurred by the victim of overenforcement.[98] When a preemptive bar causes only slight inconvenience or can be overrided easily, overenforcement may pose little danger.

As an abstract matter, overenforcement through preemption might be be more tolerable than wrongful convictions for several reasons. First, criminal punishment is generally a more substantial penalty than the inability to engage in a particular course of conduct. Criminal punishment can carry significant stigma, and imprisonment, in particular, obstructs the prisoner's ability to do just anything at all. Second, overenforcement through digital preemption would be less likely to result from prejudice or corruption, since it would flow from a digital algorithm rather than human discretion. Third, wrongful preemption might be corrected relatively easily. Software updates could fix systemic problems while an appeals process could correct specific mistakes and identify problems requiring larger updates. However, this is subject to the existence of an expedient system of review

We can find guidance in this difficult area by reference to the doctrine of preliminary injunctions. Preemptive systems function much like preliminary injunctions. They are like injunctions because they block a a person from engaging in a course of conduct. They are

[97] See Dershowitz, supra note 11, at 232-33.

[98] See, e.g., Madeline Morris, After Guantanamo: War, Crime, and Detention, Harv. L. & Pol'y Rev. (2009) ("Is it really smart to release an individual shown by 'clear and convincing evidence' (the standard of proof, one step below 'reasonable doubt,' often used in civil cases) to have attempted a nuclear attack or a release of smallpox virus?")

preliminary because they take force through a brief assessment rather than a full hearing on the merits.

Preliminary injunctions are not awarded lightly,[99] largely due to the risk of false positives—decisions to enjoin conduct that is not in fact unlawful. In a recent Supreme Court decision involving military sonar technology,[100] the Court held that preliminary injunctions are appropriate when the party seeking the injunction is "likely to succeed on the merits" and would be "likely to suffer irreparable harm" if the injunction were not issued.[101] Furthermore, the party seeking the injunction must show that "the balance of equities tips in his favor" (a requirement that will not be discussed here) and that the injunction would be in the public interest.[102] This doctrine is instructive in thinking about preemptive techniques.

In the context of preemption, the requirement of likely success on the merits would require preemption techniques to accurately identify unlawful conduct more often then they make mistakes.[103] The irreparable harm requirement would bar preemption except when the conduct at issue was dangerous and hard to redress through alternate law enforcement

[99] See Winter v. Natural Resources Defense Council, 129 S.Ct. 365, 376 (2008) ("A preliminary injunction is an extraordinary remedy never awarded as of right. In each case, courts must balance the competing claims of injury and must consider the effect on each party of the granting or withholding of the requested relief." (internal quotation narks, citations omitted)).

[100] Id. The plaintiffs sought to enjoin the Navy's use of sonar due to the Navy's failure to conduct an environmental impact statement.

[101] Id. at 374.

[102] Id.

[103] But see Dataphase Systems v. CL Systems, 640 F.2d 109, 113 (8th Cir. 1981) (cautioning against a "wooden application of the probability test").

techniques.[104] Yet, the standard is not as high as it might be. For example, the doctrine does not require that the plaintiff show that they are nearly certain to prevail.

To see how these factors might guide analysis of a preemptive technique, suppose that someone has been prevented from driving by an ignition interlock system that accurately measures her Blood Alcohol Level to exceed 0.08. In almost every instance, if the person were to drive, the state would be "likely to succeed on the merits" of a drunk driving prosecution. Furthermore, drunk driving threatens "irreparable harm" in danger to human life. Admittedly, if we focus on a particular act of drunk driving, the act may not be *likely* to result in irreparable harm. On the other hand, when taken together, it is beyond question that the acts of drunk driving prevented by an ignition interlock mandate would otherwise result in a great deal of irreparable harm. Overall, it seems fair to say that the harm requirement is satisfied here.

Finally, under preliminary injunction doctrine, the court must assess the public interest.[105] For example, in the military sonar case, the Court examined the negative consequences for the public of preventing military sonar experiments.[106] In the drunk driving example, the public interest might include the harm to the public from intrusion on liberty and benefit of reducing car accidents for public health and transportation.

In other contexts, the public interest requirement may caution against preemption. For example, this requirement would urge extreme caution when dealing with preemptive techniques that burden free speech. The constitutional bar on censorship is motivated at least as much by

[104] Due to the nature of preemption, these inquiries would have to be undertaken generally, not in reference to any particular circumstances. Preemptive code would be implemented before particular situations occurred.

[105] See Winter, 129 S. Ct. at 364.

[106] Id. at 378.

society's interest in a free trade of ideas as the individual's interest in self-expression.[107] And, in the doctrine of "prior restraints," courts have long recognized that preemptive bars on speech are highly suspect.[108]

B. Stasis

Preemption carries a second, somewhat more speculative risk: When preemption is used to enforce a law, the law may be immune from several traditional processes of change.[109] Unlike traditional law enforcement, preemption does not require the participation of citizens, public officials, or judges. And without arrests or trials, preemption takes place largely in private. As a result, laws enforced through preemption be much less likely to encounter repeal or amendment as compared to laws enforced through traditional means.

Stasis will of course be troubling to anyone who believes that the substantive law is incorrect. For example, an opponent of current copyright laws should oppose YouTube's preemptive enforcement policy both because it is more effective than other enforcement methods and because, as a result of this effectiveness, the law will be less likely to change.[110] Furthermore, regardless of the merits of a legal prohibition, stasis may be troubling in itself, especially in the circumstances described in the final part of this section.

---

[107] See Abrams v. U.S., 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) ("[T]he ultimate good desired is better reached by free trade in ideas.")

[108] See, e.g., Nebraska Press Assn. v. Stuart, 427 U.S. 539 (1976).

[109] This section is most closely linked to Zittrain's concern about the erosion of "Bulwarks Against the Government." See id. at 118 ("The rise of tethered appliances significantly reduces the number and variety of people and institutions required to apply the state's power on a mass scale. It removes a practical check on the use of that power. It diminishes a rule's ability to attain legitimacy as people choose to participate in its enforcement, or at least not stand in its way.") It is also connected to his discussion of "The Undesirable Collapse of Conduct and Decision Rules." See id. at 122 (examining "one's right to flout the law").

[110] Zittrain opposes preemption of copyright laws for at least the first of these reasons. Future, supra note 3, at 111.

As a final preliminary note, the problem of stasis is not, in theory, unique to *digital* preemption. As I will show, the phenomenon can arise whenever a law is enforced through preemption so effectively as to nearly eliminate violations of the law across an entire jurisdiction.[111] However, non-digital methods of preemption have rarely achieved this level of effectiveness. This may be why stasis has not been explored in the criminology literature. Stasis demands our attention now due to the potentially overwhelming effectiveness of digital preemption.

1. The role of public officials and citizens in enforcement

Traditional law enforcement requires the participation of many people, including police, prosecutors, judges, and ordinary citizens. These people can change how law is applied or, in the case of judges, change the substantive law itself.

At several junctures in the traditional law enforcement model, police, prosecutors, and other public officials have an opportunity to shape how the law is applied.[112] Police and prosecutors exercise their discretion both in individual cases and through systematic policies. For example, pursuant to an October 2009 memorandum, federal prosecutors will no longer prosecute people who use marijuana for medicinal purposes in 14 states where such use is not prohibited under state law.[113] The memorandum amounts to a change in federal law on marijuana use in these 14 states.

---

[111] In fact, a tendency towards stasis might even arise from traditional deterrence if it is powerful enough to prevent nearly all violations.

[112] Angela J. Davis, Arbitrary Justice: The Power of the American Prosecutor 6 (2007) ("Discretion is the hallmark of the criminal justice system, and officials at almost every stage of the process exercise discretion in the performance of their duties and responsibilities.").

[113] David Stout and Solomon Moore, U.S. Won't Prosecute in States that Allow Medical Marijuana, N.Y. Times, October 19 2009

While the marijuana decision has raised controversy,[114] other systematic uses of prosecutorial discretion are generally accepted. Police and prosecutors often seem to work in tandem in such situations. For example, many states have laws prohibiting adultery.[115] Yet, it is generally accepted that police will not investigate and prosecutors will not prosecute violations of these laws.[116] Consequently, police and prosecutors have essentially changed the law to better conform to modern social norms.[117] For example, in striking down state prohibitions on sodomy, the Supreme Court noted that such prohibitions were rarely enforced.[118]

Citizens, too, participate in traditional law enforcement in important ways.[119] Most obviously, citizens help police and prosecutors enforce the law by providing information. But the public can also help repeal a law simply by refusing to obey it. Without widespread compliance, the government often struggles to detect and punish rampant violations and law enforcement can become prohibitively difficult.[120] Again, adultery laws are illustrative. Even if the state wanted to enforce these laws, people might continue to violate them in significant

[114] See id. (describing criticism of the marijuana policy).

[115] See Gabrielle Viator, The Validity of Criminal Adultery Prohibitions after Lawrence, 39 Suffolk U. L. Rev. 837, 843 ("Adultery remains a crime in twenty-three states with punishment varying significantly by jurisdiction.").

[116] See Richard Posner, Sex and Reason 260-61 (Harvard University Press, 1992).

[117] To see that this is a transformation of the law, adopt the perspective of the Holmesian "bad man."

[118] Lawrence v. Texas, 539 U.S. 558, 569 (2003).

[119] See Mulligan, supra note 15, at 48.

[120] See David E. Kyvig, Repealing National Prohibition 22 (2000) (using Prohibition to argue that when enough citizens are determined not to follow a law, "it cannot be imposed upon them"). See also Arthur R. Hadley, Law Making and Law Enforcement, Harper's Magazine, Nov. 1925 ("Conscience and public opinion enforce the laws… the police suppress the exceptions... If any considerable number of citizens who are habitually law-abiding think that some particular statute is bad enough in itself or dangerous enough in its indirect effects to make it worthwhile to block its enforcement, they can do so.")

numbers.[121] Along with public officials' own aversion to enforcing these laws, this probable lack of compliance helps explain why adultery bans are not enforced and have been repealed in many states.[122]

America's experience during Prohibition illustrates how citizens can exert significant pressure to repeal a law through noncompliance, even when the government strongly stands behind the law. The Federal Government devoted significant resources to enforcing Prohibition. At the outset, there were over 2,000 federal prosecutions per month.[123] Yet, while the public had once supported Prohibition,[124] citizens nevertheless continued to consume intoxicating liquors. This made enforcement of Prohibition incredibly expensive. Federal officials estimated that the government would need an additional 35,000 officers to patrol coasts and borders to stop imports of alcohol.[125] By comparison, there were fewer than 6,000 police officers working in the entire city of Chicago at the time.[126] In large part because they could not afford to enforce prohibition, states started to repeal their enforcement acts in the mid 1920s.[127] Meanwhile, the federal government scaled back enforcement,[128] then repealed Prohibition. Today, copyright law may

---

[121] See Phyllis Coleman, Who's Been Sleeping in My Bed? You and Me, and the State Makes Three, 24 Ind. L. Rev. 399, 409 (1991) ("It is naïve to think that merely criminalizing sexual behavior will suppress the strongest of all biological drives.")

[122] See, e.g., Kevin Landrigan, NH Adultery Law May Be Repealed, Nashua Telegraph, Jan. 13, 2010 (describing widespread support for repealing New Hampshire's adultery prohibition in part because "the law is unenforceable").

[123] Kyvig, supra note 120, at 29.

[124] Id.at 68.

[125] Id.at 29.

[126] U.S. Census Bureau, Total Males and Females 10 Years of Age or Older Engaged in Each Selected Occupation, 1920 Census 1078, availble at http://www2.census.gov/prod2/decennial/documents/41084484v4ch10.pdf.

[127] Kyvig, supra note 120, at 29.

[128] Id.

be in a similar predicament. Often using the internet, people frequently violate copyright law, both intentionally[129] and unintentionally.[130]

This sort of noncompliance can have a similar effect as civil disobedience, though not performed with a conscious intent to bring about legal change.[131] In the face of effective preemption, however, neither general noncompliance nor civil disobedience can create such change. Imagine if the government was, in fact, able to nearly eliminate alcohol consumption during prohibition or copyright infringement today. The relevant law would be much less likely to change, at least through pressure from noncompliance.[132]

Of course, this analysis does not resolve a crucial question: Is this form of citizen participation in legal change desirable? Some might favor preemption precisely because it reduces the ability of citizens to disrupt law enforcement in this way. In the final part of this section, I will argue that this kind of participation can be highly desirable, particularly in areas where the law is unsettled.

---

[129] See Salamander Davoudi, Music Body Says 95% of Downloads Illegal as CD Sales Fall, Financial Times, January 22, 2010.

[130] See John Tehranian, Infringement Nation: Copyright Reform and the Law/Norm Gap, 2007 Utah L. Rev. 537, 547-48 (describing a professor's largely inadvertent violation of copyrights of "twenty emails, three legal articles, an architectural rendering, a poem, five photographs, an animated character, a musical composition, a painting, and fifty notes and drawings").

[131] John Rawls, The Justification of Civil Disobedience in John Arthur & William Shaw, eds, Readings in the Philosophy of Law 67 (4th ed. 2000).

[132] However, preemption may rely on intermediaries such as Internet Service Providers (ISPs). This provides some opportunity for noncompliance, as intermediaries might choose not to participate in the preemption. For example, Google recently decided not to participate in a China's program for preventing access to certain materials online. See Andrew Jacobs & Miguel Helft, Google, Citing Attacks, Threatens to Exit China, New York Times, Jan 12, 2010. For more on intermediaries, see generally Jonathan Zittrain, A History of Online Gatekeeping, 19 Harv. J. L. & Tech 253 (2005-2006) (describing regulation through intermediaries like ISPs as one of two kinds of "online gatekeeping").

2. Legal change through courts

Laws enforced through preemption might undergo significantly reduced judicial scrutiny due to the scarcity of violations. These laws would be less likely to change through judicial interpretation or common law adjudication. This section will outline this argument but then highlight several significant counterarguments.

Courts alter laws through constitutional scrutiny, statutory interpretation, and the common law mode of analysis. But courts cannot review laws that are not brought before them, usually a result of a person's violation of the law. For example, when a court invalidates a criminal law on constitutional grounds, it usually does so at the request of someone who has been prosecuted under the law. The decision might occur directly after a prohibition is enacted, as in the Supreme Court's decision to strike down a prohibition on cross burning in *R.A.V. v St. Paul*.[133] Or it might come when norms have changed after many decades, as in the Court's decision in *Lawrence v. Texas*.[134] When a court does not strike down a law, it still might change the law by invalidating part of it[135] or by interpreting it narrowly.[136]

Even when constitutional concerns are not implicated, legal rules change through the common law process. While many states have codified large sections of their law, state courts

[133] R.A.V. v. St. Paul, 505 U.S. 377 (1992)

[134] Lawrence v. Texas, 539 U.S. 558 (2003). The Lawrence court acknowledged that state sodomy prohibitions had generally existed for over 40 years, though these prohibitions were rarely enforced. Lawrence, 539 U.S. 558, 572 (2003).

[135] See, e.g., Virginia v Black, 538 U.S. 343 (2003) (striking down one provision of a law that prohibited cross-burning with intent to intimidate).

[136] See, e.g., Clark v Martinez, 543 US 371, 379 (2005) (interpreting a statute pertaining to deportation so as to "avoid constitutional doubts").

still clarify and alter portions of this law.[137] Indeed, some elements of common law may be beyond the reach of the legislature, "at least without a compelling showing of necessity or a provision for a reasonable alternative remedy."[138] Even when courts interpret statutes, they often extend, shape, or create rules in much the same way as they would when operating exclusively with common law. [139] Peter Strauss has written that the Supreme Court frequently "deploy[s] the familiar methods of the common law."[140]

Yet, there are some persuasive reasons to doubt that preemption will lead to significantly reduced judicial scrutiny. First, even without preemption, most violations of the law do not generate judicial proceedings. In the criminal context, many violators are never caught. And, of the violators that are caught, the vast majority negotiate a plea bargain.[141] Similarly, civil claims are frequently settled out of court. Given that judicial scrutiny is already relatively rare, preemption may have little real effect on the likelihood of legal change through judicial review.

Second, a law can often be challenged in court even when the challenger has not been prosecuted or penalized, as illustrated in the recent *Citizens United* case[142] and others.[143] A

---

[137] The phrase "common law" was found in 6430 federal court opinions in 2008 indexed by google scholar (probably an underestimate of the total number of uses). See, e.g., Speight v. Walters Dev. Co., 744 N.W.2d 108, 110 (Iowa 2008) ("extend[ing] [Iowa's] common law of implied warranty to cover" third party home purchasers).

[138] Pruneyard Shopping Ctr. v. Robins, 447 U.S. 74, 94 (U.S. 1980) (Marshall, concurring).

[139] See Richard Pildes, Intent, Clear Statements, and the Common Law: Statutory Interpretation in the Supreme Court, 95 Harv. L. Rev. 892, 913 (1982) (arguing that statutory interpretation, like constitutional and common law adjudication, is the "exercise of the power to 'say what the law is'"). For an example, see State v. Engle, 743 N.W.2d 592, 595 (Minn. 2008) (adopting a standard of recklessness to be applied under a Minnesota drunk driving statute).

[140] Peter L. Strauss, 2001 Daniel J. Meador Lecture: Courts or Tribunals? Federal Courts and the Common Law, 53 Ala. L. Rev. 891, 893 (2002).

[141] See Dirk Olin, Plea Bargain, N.Y. Times, September 29, 2002 (citing Professor Albert Alschuler's claim that "roughly 90 percent of convictions occur when a defendant waives the right to trial and pleads guilty").

[142] The government had not initiated any legal proceeding against plaintiff Citizens United. See Citizens United v. Federal Election Comm'n, 130 S.Ct. 876, 888 (2010) ("Citizens United… feared, however, that both the film and

person who has been barred from engaging in preempted conduct would likely have standing to challenge the substantive law or enforcement mechanism in court. As required by standing doctrine, the person will have suffered an "injury in fact"[144] in the inability to engage in the conduct. There will be a "causal connection" between the injury and the substantive law and enforcement mechanism,[145] and the injury will be redressable through monetary damages or by altering the law or enforcement mechanism.[146] For example, someone who cannot access an allegedly obscene website due to a government filtering system will likely have standing to challenge the system in court.

It is true that such a person will have less incentive to challenge the law than a criminal defendant, since the defendant is faced with criminal punishment and the victim of wrongful preemption is not. Furthermore, the preemptive victim must bear a greater cost to challenge the law than the typical criminal defendant, who need not initiate a legal proceeding and can be represented cost-free by a public defender. The government might help alleviate these problems, however. For example, Congress could guarantee a set amount of monetary damages to anyone who prevails in a claim based on wrongful preemption. This would increase the incentive to

---

the ads would be covered by [the Bipartisan Campaign Reform Act of 2002]…. Citizens United sought declaratory and injuntive relief.").

[143] See, e.g., Church of Lukumi Babalu Aye v. City of Hialeah, 508 U.S. 520 (1993) (striking down a statute on free exercise grounds when the plaintiffs had not been prosecuted or penalized for violating the statute).

[144] Lujan v. Defenders of Wildlife, 504 US 555, 560 (1992) (requiring an "an invasion of a legally protected interest which is (a) concrete and particularized… and (b) actual or imminent, not conjectural or hypothetical" (quotations, citations removed). Here, the "legally protected interested" would the ability to engage in the preempted conduct.

[145] See id. Here, the causal connection would be that the preemptive system barred the plaintiff from engaging in the conduct.

[146] See id.at 568. Here, an alteration to the preemptive system would allow the person to engage in the conduct in the future.

bring legal challenges to wrongful preemption. It will also serve to discourage overenforcement, since the government would hesitate to implement inaccurate preemption.

3. Legal change through public debate

Finally, preemption does not require public arrests or trials. Indeed, when preemption is successful, there will be neither. When a person's behavior is preempted, he or she may be the only one to know. For example, when an intoxicated person's car will not start due to an ignition interlock system, the event will take place largely in private. In contrast, when a person drives while intoxicated, the arrest and trial are often public events.[147] In general, preemption is more obscured from public view than traditional enforcement.

Public debate can be spurred by arrests and trials. In 2002, the editor and publisher of a free newspaper in Kansas City, Kansas were tried for criminal defamation,[148] a Class A misdemeanor punishable by up to a year in jail and a fine of $2,500.[149] The defendants, both disbarred lawyers, had falsely reported that the local mayor lived in a wealthy county to the south. Both were convicted.[150] The case spurred significant controversy and led legislators and the state officials to advocate repeal of Kansas' criminal defamation law.[151] Such public controversy would have been less likely to arise if the publication of the false statements had been preempted.

---

[147] In a Google News search for the week of Jan 6 – Jan 12, there were 7,590 results for "DUI." For comparison, there were 323 results for "ignition interlock," although the systems are widely ordered by state courts in drunk driving cases and subject of ongoing research.

[148] Felicity Barringer, A Criminal Defamation Verdict Roils Politics in Kansas City, Kan., N.Y. Times, July 29, 2002.

[149] K.S.A. § 21-4004; K.S.A. § 21-4502; K.S.A. § 21-4503

[150] Id.

[151] AG Backs Change in Libel Law, Lawrence Journal-World, Feb 14, 2003.

Alan Dershowitz's historical examination of crime prevention illustrates this contrast. Dershowitz describes "dual systems of criminal justice" that have operated "throughout Anglo-American history": traditional criminal law and "preventive justice."[152] Dershowitz notes that traditional criminal law has been comprehensively and accurately described by historians.[153] But preventive justice, which operated "without published opinions or appellate review," is less well understood.[154]

Additionally, preemption may exacerbate the effects of status quo bias. It has been well-documented that people generally prefer to continue the status quo, even when alternatives would provide greater utility.[155] In a world of preemption, the limits imposed by the government seem firmly entrenched in the environment and therefore may be accepted by both potential lawbreakers and observers rather than considered as objects of debate. For example, public opposition to Prohibition may have died quickly if alcohol consumption had been effectively preempted. In contrast, traditional law enforcement is disruptive. Offenders face disruption in their lives as they move through the criminal justice system. But others participate in trials or hear about them in the media, which may cause them to think critically about the law, at least occasionally.

4. Evaluating stasis

Like overenforcement, stasis will be more worrisome in some situations than in others. They key inquiry is whether the substantive law is firmly entrenched or, instead, somewhat

[152] Dershowitz, supra note 11, at 40-41.

[153] Id. at 41.

[154] Id at 41-42. Dershowitz notes that the preventive system was probably better understood in its own time.

[155] See, e.g., William Samuelson and Richard Zeckhauser, Status Quo Bias in Decision Making, 1 Journal of Risk and Uncertainty 7, 8 (1988). This is also a prominent component of Thaler and Sunstein's recommendations in *Nudge*.

unsettled. A law can be classified as unsettled when there is significant disagreement among the public about the law or the norms that underlie it. For example, laws regulating pornography are unsettled because the public disagrees about the merit of these laws.[156]

Much of the law governing cyberspace seem unsettled. We can tell that internet law is in flux because the internet itself is a relatively new medium, because legislatures and agencies are busy revising rules for the internet,[157] and because people disagree vociferously about how cyberspace should be governed.[158] This means that there is reason to doubt whether current cyberspace rules are the right ones. Copyright law on the internet seems to be especially contentious. Responding to this uncertainty, Lawrence Lessig has issued a "plea… for the common law" in cyberspace.[159] Lessig argues that we should rely on common law in this unsettled area because "many people get to say what the common law should mean, each after the other, in a temporally spaced dialogue of cases and jurisdictions."[160] This sort of broad participation and gradual change is threatened by preemption.

The benefits of flexibility in the law are not limited to the internet. Legal scholars have argued persuasively that flexibility through common law leads to more efficient rules over

[156] See, e.g., No Consensus Among American Public on the Effects of Pornography on Adults or Children or What Government Should Do About It, According to Harris Poll, Harris Interactive, October 7, 2005 (finding that fifty five percent of Americans believed pornography should be regulated while thirty four percent thought pornography should not be regulated), available at http://www.harrisinteractive.com/harris_poll/index.asp?PID=606.

[157] See, e.g., McCain Introduces Bill to Block FCC's Net Neutrality Rules, Reuters, Oct. 22, 2009, available at http://www.reuters.com/article/idUS238174038020091023?rpc=64.

[158] See, e.g., Zogby Survey Finds U.S. Adults Committed to High Tech Economy, Zogby International, June 8, 2009 (finding that 30% of Americans "believe the Internet should be regulated as television is" and 32% "believe any regulation or blocking of Internet video is unconstitutional"), available at http://www.zogby.com/News/ReadNews.cfm?ID=1706.

[159] Lawrence Lessig, The Path of Cyberlaw, 104 Yale L.J. 1743, 1745 (1995).

[160] Id.

time.[161] Furthermore, flexibility allows the law to conform to changing social norms. For example, as norms about adultery have changed in the last hundred years, the law enforcement system has permitted—and indeed, forced—prosecutorial practice to change with them.

One might question whether such change is desirable. After all, if one is absolutely certain that a legal rule is correct, why should one embrace an enforcement model that might someday contribute to its repeal or amendment? Oliver Wendell Holmes and Ronald Dworkin have provided powerful answers. In his famous discussion on free speech and the marketplace of ideas,[162] Holmes starts by noting that "if you have no doubt of your premises," then it is "perfectly logical" to suppress opposing speech.[163] Yet, Holmes insists that we can never be so certain of our beliefs and must allow the "competition of the market" to reveal the truth.[164] The mechanisms of legal change discussed in this section are part of that market.

Dworkin applies this concept directly to law in the context of civil disobedience. Dworkin argues that there are many examples of "doubtful law" and that legal authorities, including the Supreme Court, are sometimes wrong.[165] Even within short periods, courts have often realized that their previous decisions were legally or morally incorrect.[166] Furthermore, in the long run, change in social norms and legal rules has generally led to a more just society. As

---

[161] See George L. Priest, The Common Law Process and the Selection of Efficient Rules, 6 J. Legal Stud. 65 (1977); Paul H. Rubin, Why is the Common Law Efficient?, , 6 J. Legal Stud. 51 (1977).

[162] Abrams v. United States, 250 U.S. 616, 630 (1919).

[163] Id.

[164] Id.

[165] Ronald Dworkin, Civil Disobedience in John Arthur & William Shaw, Reading in the Philosophy of Law 8 (2nd ed. 1993) (1984).

[166] For Dworkin's example, compare Minersville School Dist. v. Gobitis, 310 U.S. 586 (1940) (upholding a school board's requirement that school children salute the flag) with West Virginia Bd. of Ed. v. Barnette, 319 U.S. 624 (1943) (striking down a nearly identical statute).

Dworkin notes, civil disobedience can provide a valuable indication that the law is out of sync with common belief or morality.[167] Other forms of participation by citizens and public officials can play the same role.

Yet, there are many areas in which the law is not "doubtful." In these areas, legal rules are supported by established norms and seem unlikely to change; there are few suggestions that different rules might be more just or efficient. For example, laws prohibiting theft of property are well-settled. So too are laws prohibiting physical violence and drunk driving. Perhaps this helps explain why locks, metal detectors, and ignition interlock systems seem more acceptable than other forms of preemption. Even in cyberspace, many laws are fairly settled. For example, prohibitions on identity theft are not typically challenged. Certainly, even well-settled rules might naturally change over time. But given the low likelihood of this and the existence of alternative, if less effective, routes of change,[168] the state can use preemption in these areas with little risk. For example, stasis will not be much of a problem when preemption is used to enforce laws that protect people or property from direct harm.

III. Deciding whether and how to preempt: suggestions for lawmakers

This article has highlighted two risks of digital preemption and argued that these risks carry varying force depending on the circumstances. These risks should be weighed against the possible advantages of digital preemption. Previous work has not devoted much attention to these advantages.[169] This may be in part because the key advantage of preemption seems fairly

[167] Dworkin, supra note 167, at

[168] Even when a rule is enforced through preemption, the legislature or administrator might still change the rule. For example, rules proscribing which items can be brought into an airport have changed while being enforced preemptively.

[169] Zittrain writes that "[i]f one could wave a wand and make it impossible for people to kill each other, there might seem little reason to hesitate." Future, supra note 5, at 110. But he has little to say about the benefits of non-magical preemptive techniques.

obvious: preemption could greatly limit the occurrence of unlawful conduct.[170] In this respect, preemption would be an improvement over traditional law enforcement, particularly in cyberspace, which has proved somewhat difficult to regulate effectively using traditional law enforcement.[171]

Preemption will be especially attractive in the widely recognized circumstances in which traditional law enforcement is least effective. For example, when even one violation of a law would be catastrophic, we may be loathe to rely on traditional law enforcement. The deterrence model "presupposes society's ability (and willingness) to withstand the blows we seek to deter…"[172] Even among non-catastrophic crimes, some harms are much more endurable than others. On the internet, for example, identity theft may be less tolerable than copyright infringement.[173] Second, enforcement through deterrence works poorly when "some offenders are not rational, often enough to matter."[174] We may favor preemptive approaches to terrorism in part because we believe that the state cannot deter someone willing to die in the course of the crime.

---

[170] As discussed in Section I.C.2, preemption would usually not eliminate occurences of the targeted crime, but it could significantly increase the cost of that crime, making it less commonplace. But note that displacement may limit this benefit.

[171] See, e.g., remarks by President Barack Obama on Cyber-Security, printed in N.Y. Times, May 29, 2009 ("Millions of Americans have been victimized, their privacy violated, their identities stolen, their lives upended, and their wallets emptied. According to one survey, in the past two years alone cyber crime has cost Americans more than $8 billion.").

[172] Dershowitz, supra note 11, at 7.

[173] See remarks by President Barack Obama on Cyber-Security, supra note 171. See also Beth Healy, Credit Agencies Lag on Errors, Fraud, Boston Globe, Dec. 28, 2006 (quoting an identity theft victim as saying, ""[i]t literally ruins your life").

[174] David M. Kennedy, Deterrence and Crime Prevention: Reconsidering the Prospect of Sanction 17 (2008).

Even when preemption is no more effective than traditional law enforcement, it may be more efficient. Traditional law enforcement requires police, legal proceedings, and prisons, each of which involves substantial costs.[175] While research and development of effective preemptive techniques might not be cheap, it could produce significant savings.

If the government embraces digital preemption, legislatures should take steps to minimize the risks of overenforcement and stasis. In the area of overenforcement, legislatures should refuse to permit preemption of laws that are too complex to apply though code, such as anti-obscenity regulations. Furthermore, legislatures should ensure that there are effective systems in place to review possble errors. Legislatures might require any agency that uses a preemptive technique to provide avenues of review. If a state Bureau of Motor Vehicles administers an ignition interlock program, for example, it should also be required to establish a system of review. The agency would be responsible for providing corrective remedies, such as fixing defective interlock systems. As either a supplement or alternative to agency review, the legislature should ensure avenues fopr judicial review of preemption.[176] And, to ensure that victims of erroneous preemption come forward with their claims, legislatures should consider providing for mandatory monetary damages, as discussed in Section II.B.2.

Judicial review of digital preemption will also help to alleviate the risk of stasis. But it may not be sufficient. Consequently, legislatures should prevent the government from enforcing unsettled laws through digital preemption. For example, the government should not require

[175] Solomon Moore, Prison Spending Outpaces All but Mediciad, N.Y. Times, March 2, 2009 (noting that American states spent $47 billion on prisons in 2008 and that prison spending "is outpacing budget growth in education, transportation and public assistance").

[176] As noted in Section II, victims of erroneous preemption likely already have standing to challenge preemption in court.

Internet Service Providers to mimic YouTube's copyright removal policy for all content uploaded through their servers.

Additionally, government should avoid creating indirect incentives for private parties to preempt when there are significant overenforcement or stasis concerns. Such incentives will arise if creators of digital devices or software face liability for their users' crimes. When internet companies denied service to Wikileaks in late 2010, their actions were motivated, at least in part, by this kind of indirect pressure.[177] Thus, legislatures who want to limit occurences of preemption should consider providing immunity for technology companies.

Finally, legislatures might go even further and prohibit private preemption. This propsect raises complex questions which cannot be addressed in this article. For now, it must suffice to say that legislatures should think carefully about whether such action is necessary in light of market pressures and whether the benefits of preemption would justify intrusion on the ability of companies to design products as they see fit.

IV. Conclusion

Oliver Wendell Holmes penned one of the most memorable phrases in American legal scholarship when he wrote, "The life of the law has not been logic: it has been experience."[178] But technology may yet alter the balance in law between logic and experience, as it has in other parts of our lives. Increasingly, for example, products are manufactured not by people guided by their experience but rather by machines, operating according to set logical algorithms. Most

[177] See, e.g., Apple Removes iPhone Wikileaks App From iTunes, BBC News, Dec. 22, 2010 (noting that Apple acted because "Apps must comply will all local laws and may not put an individual or targeted group in harms way"), available at http://www.bbc.co.uk/news/technology-12059577. Amazon may or may not have evicted Wikileaks from its servers due to government pressure. Amazon claimed that it acted due to violations of its terms of service, but Wikileaks retorted, "Amazon's press release does not accord with the facts on public record. It is one thing to be cowardly. Another to lie about it." Compare Geoffrey Fowler, Amazon Says Wikileaks Violated Terms of Service, Wall Street Journal, Dec. 2, 2010 with Spencer Dalziel, Wikileaks Calls Amazon a Liar Over Government Pressure, The Inquirer, Dec. 6, 2010.

[178] Oliver Wendell Holmes, The Common Law 1 (1881).

observers see this as progress, but others bitterly disagree. This debate echoes in discussions of digital preemption. As Holmes reminds us, the law relies on—and, perhaps, *must* include—human discretion. This means that there is risk associated with technological bars to crime. But it does not mean that we should dismiss such approaches entirely. Instead, we must navigate this uncertain territory with care.