Richmond Journal of Law and Technology

Volume 14 | Issue 4 Article 4

2008

Perfect Enforcement Of Law: When To Limit And When To Use Technology

Christina M. Mulligan

PERFECT ENFORCEMENT OF LAW: WHEN TO LIMIT AND WHEN TO USE TECHNOLOGY

By: Christina M. Mulligan*

Cite as: Christina M. Mulligan, *Perfect Enforcement of Law: When to Limit and When to Use Technology*, 14 RICH J.L. & TECH. 13 (2008), http://law.richmond.edu/jolt/v14i4/article13.pdf.

I. INTRODUCTION

[1] Road safety cameras can photograph your car running red lights.[1] Some bars record information on driver's licenses to establish that their patrons are old enough to drink.[2] The Recording Industry Association of America (RIAA) uses automated web crawlers[3] to try to find illegal copies

* Harvard Law School '08. Beginning in September 2008, the author will be an associate at Winston & Strawn LLP in San Francisco, CA. She would like to thank Jonathan Zittrain for his thoughtful comments and tremendous help crystallizing this article, as well as Peter Koellner of the Harvard Philosophy Department and Jim Waldo of Sun Microsystems and the Harvard Computer Science Department. Thanks are also due to the many whose scholarship, lectures, or conversation influenced and inspired portions of this work, including Randy Barnett, Terry Fisher, Allan Friedman, Abel Roasa, Michael Smith, Mark Tushnet, and all those who took part in Harvard's Computer Science 199r course in Spring 2007.

[1] *See* Tom Harris, *How Red-Light Cameras Work*, Howstuffworks.com, http://auto.howstuffworks.com/red-light-camera.htm/printable (last visited Nov. 10, 2007).

[2] *See* Jennifer 8. Lee, *Welcome to the Database Lounge*, N.Y. TIMES, Mar. 21, 2002 at G1, *available at* http://www.nytimes.com/2002/03/21/technology/circuits/21DRIV.html.

[3] A web crawler is a program that methodically scans or "crawls" through Internet pages to create an index of the data it is looking for. *See* WiseGeek.com, What is a Web Crawler?, http://www.wisegeek.com/what-is-a-web-crawler.htm (last visited June 4, 2007).

of mp3s,[4] and iTunes embeds personal identifying information in the tracks of every song you buy.[5]

[2] Both public and private parties are harnessing technology to enforce law more accurately and efficiently, approaching a "perfect enforcement" of some laws. These measures are often more accurate and less costly than hiring dozens of investigators and police officers to do similar work.[6] However, the invasiveness and omnipresence of these measures can make those who are monitored feel downright uncomfortable.

[3] "Uncomfortable" is not much to hang your hat on. Those who are quick to express concern that "they" are watching us can appear alarmist. Yet, many feel that there is a real and very significant cost to using technology to enforce laws. But what is it?

[4] A few legal writers, notably Daniel Solove,[7] Eugene Volokh,[8] and Jonathan Zittrain,[9] have discussed the use of perfect law enforcing technologies. Yet, relatively little has been written on the subject. There are many kinds of law enforcing technologies, and each raises a variety of concerns. This article provides a framework which can be used to determine the wisdom of using a technology to enforce law by explaining

---

[4] *See* RIAA, *Worldwide Music Industry Coordinates Its Strategy Against Piracy*, Oct. 28, 1999, http://www.riaa.com/newsitem.php?news_year_filter=&resultpage=114&id=323A12AC-539B-2909-BC1F-654DD1644E9E (last visited Apr. 10, 2008); *see also* Declan McCullagh, *RIAA Apologizes for Erroneous Letters*, CNETNews.com, May 13, 2003, http://news.com.com/2102-1025_3-1001319.html (last visited Apr. 10, 2008) [hereinafter McCullagh, Erroneous Letters].

[5] *See 'Personal Data' in iTunes Tracks*, BBC NEWS, June 1, 2007, http://news.bbc.co.uk/2/hi/technology/6711215.stm (last visited Apr. 10, 2008).

[6] *See e.g.,* Posting of Randy Picker to the University of Chicago Law School Faculty Blog, http://uchicagolaw.typepad.com/faculty/2006/05/more_driving_do.html (May 26, 2006, 15:59 CST); Posting of Daniel J. Solove to Concurring Opinions, http://www.concurringopinions.com/archives/2005/10/do_we_really_wa_1.html (Oct. 12, 2005, 00:15 EST).

[7] *See* Solove, *supra* note 6.

[8] *See* Eugene Volokh, *Traffic Enforcement Cameras*, WALL ST. J., Mar. 22, 2002, at A22, *available at* http://www.law.ucla.edu/volokh/cameras.htm.

[9] *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET — AND HOW TO STOP IT 103-17 (2008).

the several types of perfect enforcement and analyzing the concerns raised by their use.

[5] When considering whether to use technology to enforce law, a decision-maker should make four determinations. First, is the aversion to using the technology an aversion to the method of enforcing the law or a disagreement with the underlying substantive law? Second, will the technology effectively enforce the law? Third, is the use of the technology constitutional? And finally, does the technology trigger any other philosophical concerns?

[6] In some cases, the use of technology will plainly be justified or unjustified. More often, the appropriateness of using technology will depend on the particular facts and circumstances of its use. Even when these grey situations arise, this article's structure and explanation of concerns can be used as a means to help legislators, law enforcers, and policymakers make more informed decisions about when technology should be used to enforce law.

II. WHAT KIND OF PERFECT ENFORCEMENT?

[7] "Perfect enforcement" can come in several forms. This article is principally concerned with two, perfect prevention and perfect surveillance, but will discuss a third, perfect correction, briefly.

[8] A technology which "perfectly prevents" a law violation preempts the law violation entirely.[10] Perfect prevention technology includes Digital Rights Management ("DRM") systems, which prevent access and copying of media. A perfect prevention technology can also be indirect; for example government systems designed to identify terrorist attacks before they take place qualify as a prevention technology.

[9] A "perfect surveillance" technology would not interfere with the act of violating the law but would detect every instance of its violation.[11]

[10] Jonathan Zittrain has identified this type of perfect enforcement by another name. *Id.* at 108 (identifying "preemption" as a type of perfect enforcement).

[11] *Id.* at 109-10. Michael Adler's "perfect search" would also be an example of a technology designed to perfectly punish. *See* Michael Adler, Note, *Cyberspace, General*

Technologies which aspire to "perfectly survey" include red light traffic cameras and the RIAA's web crawlers. Unlike DRM, the web crawlers do not interfere with the copying or distribution of media; they merely identify the source of the media. The RIAA then uses the information the web crawler discovered to file a law suit against providers of the illegally copied media.[12]

[10] Other types of perfect enforcement which are not considered at length in this article include what Jonathan Zittrain terms "specific injunction"[13] but which might more broadly be called "perfect correction." Perfect correction is possible when a piece of technology continues to communicate with its manufacturer; examples include Digital Video Recorders (DVRs) or computer software that is set to receive automatic updates.[14] Perfect enforcement by correction would occur if a manufacturer retroactively "undid" harms after their occurrence, either by court order or its own volition.[15] A recent example of this was the remote reprogramming of Apple iPhones which had been altered to work on multiple mobile networks.[16] Another example is *TiVo, Inc. v. Echostar Communications Corp.*, in which a district court ordered the company Echostar to stop most of the DVR boxes it had already sold from functioning because they infringed patents owned by TiVo.[17]

[11] This article is primarily concerned with perfect prevention and punishment, although many concerns raised about perfect prevention are also relevant to perfect correction.

Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search, 105 YALE L.J. 1093 (1996).

[12] *Worldwide Music Industry Coordinates Its Strategy Against Piracy*, *supra* note 4.

[13] ZITTRAIN, *supra* note 9, at 108-09.

[14] *Id.*

[15] *Id.* at 109.

[16] *See Apple iPhone Warning Proves True*, BBC NEWS, Sept. 28, 2007, http://news.bbc.co.uk/2/hi/Technology/7017660.stm (last visited Apr. 10, 2008).

[17] *TiVo, Inc. v. EchoStar Commc'ns Corp.*, 446 F. Supp. 2d 664 (E.D. Tex. 2006), *aff'd in part, rev'd in part, remanded*, 516 F.3d 1290 (Fed. Cir. 2008). For an extended discussion of *TiVo, Inc. v. Echostar Communications Corp.*, and its implications, see ZITTRAIN, *supra* note 9, at 103–04, 108.

III. AVERSIONS TO THE UNDERLYING SUBSTANTIVE LAW

[12] As mentioned in the introduction, the idea of perfect law enforcement makes people nervous. But is this nervousness misplaced? Some of the discomfort comes not from concerns about privacy or government power, but from a concrete disagreement with the substance of laws themselves. Consider how many individuals consume alcohol at least once before they are twenty-one, smoke marijuana, break the speed limit, or pirate media. Many of these lawbreakers are generally law-abiding and productive members of society. Furthermore, many of these lawbreakers are also principled about their lawbreaking; they believe the laws are poorly crafted or simply wrong and do not consider themselves immoral.

[13] Thus, it is unsurprising when, for instance, someone in favor of the legalization of marijuana is opposed to random drug testing. As it has not been politically feasible to repeal anti-drug laws, proponents of marijuana use may find more political success by opposing drug testing on the grounds that it is a violation of privacy. Their objection to testing may have little if anything to do with privacy and everything to do with their opposition to the substance of anti-drug laws. In cases of this type, aversion to technology can merely be a proxy for aversion to the law.

[14] Opposition to a technology can also be inspired when individuals oppose only some enforcements of a law. In 2000, the Hawaii transportation department began using cameras mounted on vans to catch anyone driving six or more miles over the speed limit.[18] One journalist observed, "it became possibly the most hated public policy initiative in Hawaii's history, almost uniformly disliked, even by those who thought it actually worked."[19] The program was cancelled in 2002, largely due to public outcry.[20] Afterwards, traffic violations were detected the old-fashioned and less-perfect way. Daniel Solove hypothesized that the outcry could be explained by individuals' ambivalent views towards

[18] *See* Solove, *supra* note 6.
[19] Mike Leidemann, *Few Saying Aloha to Van Cams Fondly*, HONOLULU ADVERTISER, Apr. 14, 2002, *available at* http://the.honoluluadvertiser.com/article/2002/Apr/14/ln/ln05a.html.
[20] *Id. See also* Solove, *supra* note 6.

speeding laws.[21] While people generally agree with speeding laws, they also believe there are many occasions when it is permissible to violate them.[22]

[15] In contrast to the above examples, Eugene Volokh has suggested that "broader and more evenhanded enforcement will generally (not always, but usually) lead to improvements in the law. If lots of citizens get pulled over for speeding, and the limit also ends up making everyone else drive too slowly, City Hall will react."[23] Volokh's vision of using better enforcement to fuel the revision of poorly crafted laws is plausible but may not always come to pass. Few who hope for a bright future in politics will risk fallout from suggesting that maybe speeders, amateur music pirates, or those who do not wear seatbelts should not be reprimanded. While some very unpopular laws may be changed, politicians may avoid altering controversial laws for fear of losing their own popularity in a public relations mishap. On the other hand, avoiding the use of an enforcement technology because the public does not fully agree with a law smacks of absurdity, especially as it will result in a more random portion of the lawbreaking population being caught.[24]

[16] Determining whether enforcement technologies should be opposed if a law is unjust is beyond the scope of this article. However, as the discussion in this article progresses, one should be careful not to conflate a concern about a law with a concern about an enforcement technology. Separating these concerns will allow objections to the technology to be

[21] Solove, *supra* note 6.
[22] *Id.*
[23] Eugene Volokh, Questions Following *Traffic Enforcement Cameras*, http://www.law.ucla.edu/volokh/
cameras.htm (last visited June 18, 2007).
[24] While beyond the scope of this Article, in cases where a law is generally just, it may be wise to add a human, discretionary element into a system of near-perfect enforcement. For example, Hawaii could keep its "traffic vans," but instead of ticketing everyone who drove six miles over the speed limit, an individual would have to make an independent judgment about whether the ticket was justified. Thus, those speeding to keep up with the flow of traffic or on a virtually empty road could be spared, but those dangerously zigzagging between lanes or traffic would be punished more often. This exercise in discretion will fit better with the public's conception of a fair application of the law, and the more targeted enforcement will result in greater fairness and punishment of those who deserve reprimand.

made more clearly by taking the focus off the substance of the law and placing it on the law enforcement method itself.

IV. LOGISTICAL CONCERNS

[17] If technology were always accurate and lawmakers could always foresee the effects of their decisions, one might be very tempted to embrace perfect enforcement of law. But this utopia is not the world we live in. Computer programs can make mistakes, laws can be unjust, and even the best laid plans can have horrific, unintended side effects. Even if using technology to enforce law were a good idea in theory, does it have a shot in practice? This section will discuss the logistical objections to using technology to enforce law, by identifying situations when using technology to enforce law should be avoided.

A. FEASIBILITY

[18] In contrast to the examples in the previous section, there are some areas of law where general consensus exists. Almost everyone wants to prevent terrorist attacks and supports some kind of government action to prevent them. With stakes so high and emotions so volatile, the idea of finding terrorists by analyzing transactional data is appealing. Yet, law enforcers must realistically assess if their goals are possible before spending tax dollars and aggregating personal information (two activities which, we will stipulate, are undesirable standing alone). Consider, for example, some of the government programs following the attack on the World Trade Center in 2001.

[19] After the terrorist attacks of September 11, 2001, many suggested that the attacks could have been prevented if American intelligence agencies could have better "connected the dots."[25] The attackers had acted suspiciously before the hijackings — taking flight lessons, purchasing last-minute one-way plane tickets using cash, and participating in suspicious

[25] "Certain agencies and apologists talk about connecting the dots, but one of the problems is to know which dots to connect." Remarks as prepared for delivery by Dr. John Poindexter, Director, Information Awareness Office of DARPA, at DARPATech 2002 Conference (Aug. 2, 2002), http://www.fas.org/irp/agency/dod/poindexter.html (last visited Apr. 10, 2008).

banking activity.[26] Looking backwards in time, it is easy to see how these extremists could have been planning a terrorist attack. But could an attack be anticipated by looking forward?

[20] There is a *prima facie* sense that the September 11th hijackers could have been identified and linked to one another. Hijackers Nawaq Alhamzi and Khalid Al-Midhar bought tickets to fly on American Airlines Flight 77 (which was flown into the Pentagon) using their real names.[27] Both were on the State Department/INS watch list called TIPOFF and both were sought by the FBI and CIA as suspected terrorists because they had been seen at a meeting with other terrorists in Malaysia.[28] From their identities, authorities could have discovered three more of the hijackers.[29] One shared an address with Alhamzi and also bought a seat on American Airlines Flight 77.[30] More importantly, authorities might have discovered Mohamed Atta and Marwan Al-Shehhi, who shared an address with Al-Midhar and who bought tickets on the two flights which flew into the World Trade Center towers.[31]

[21] Two systems of particular relevance were proposed to anticipate terrorist activity: the more modestly-aimed Computer Assisted Passenger Pre-screening System II ("CAPPS II")[32] and the grander Total Information Awareness ("TIA").[33] These programs were attempts at perfect prevention, designed to anticipate criminal activity and more-perfectly prevent it.

[22] The CAPPS II system would have airlines ask passengers for four pieces of information: full name, date of birth, home address, and home

---

[26] MARKLE FOUNDATION TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE, PROTECTING AMERICA'S FREEDOM IN THE INFORMATION AGE 28 (Oct. 2002), *available at* http://www.markle.org/downloadable_assets/nstf_full.pdf.
[27] *Id*.
[28] *Id*.
[29] *Id*.
[30] *Id*.
[31] *Id.*
[32] Press Release, Homeland Security, Fact Sheet: CAPPS II at a Glance (Feb. 12, 2004), *available at* http://www.dhs.gov/xnews/releases/press_release_0347.shtm.
[33] *See Military Intelligence System Draws Controversy*, CNN.com, Nov. 20, 2002, http://archives.cnn.com/
2002/US/11/20/terror/tracking/ (last visited Apr. 10, 2008).

telephone number.[34] With this information, the system would "conduct a risk assessment" using "commercially available data and current intelligence information" to determine if a passenger is "no risk, unknown or elevated risk, or high risk."[35] While the phrase "commercially available data" is not explained, it likely includes the kind of information available from private corporations such as ChoicePoint, which aggregate and sell records of an individual's criminal activity, education, financial history, employment, and residences, as well as other information.[36]

[23] According to several officials who worked closely on CAPPS II, but who declined to speak publicly about it, officials first "sought to identify passengers who were not 'deeply rooted' in a community," moving often or lacking an established credit history.[37] But the system produced too many false positives, identifying many airline passengers as "risky" who were little threat.[38] "I am just not prepared to say that because someone can't get a mortgage, they are a terrorist threat to an airplane," said a former official, speaking to the Washington Post on condition of anonymity.[39] "These data aggregator products are used today in the financial world to identify certain things, and they're not designed to identify potential terrorist threats."[40]

[24] Of greater aspirations and greater failure was the Total Information Awareness program ("TIA") (also known as Terrorism Information Awareness), for which Congress eliminated funding in the Fall of 2003.[41]

---

[34] Press Release, *supra* note 32.
[35] *Id.*
[36] *See* ChoicePoint, http://www.choicepoint.com (last visited June 4, 2007); ChoiceTrust, http://www.choicetrust.com (last visited June 4, 2007).
[37] Arshad Mohammed & Sara K. Goo, *Government Increasingly Turning to Data Mining*, WASH. POST, June 15, 2006, at D03, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html.
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1460 (2004). The law which eliminated funding stated,

> (a) Notwithstanding any other provision of law, none of the funds appropriated or otherwise made available in this or any other Act may be obligated for the Terrorism Information Awareness Program:

Unlike CAPPS II, which assessed the risk of particular subjects, TIA attempted to use a "pattern based" search to find potential terrorists. Pattern-based searches look for information which matches or departs from a pattern, instead of searching for instances of a particular individual's activity.[42] TIA's goal was to detect terrorist activities from the billions of commercial transactions occurring in society every day.[43]

[25] While many were concerned with whether TIA would violate an individual's privacy,[44] few expressed concern about whether the program

> Provided, [t]hat this limitation shall not apply to the program hereby authorized for Processing, analysis, and collaboration tools for counterterrorism foreign intelligence, as described in the Classified Annex accompanying the Department of Defense Appropriations Act, 2004, for which funds are expressly provided in the National Foreign Intelligence Program for counterterrorism foreign intelligence purposes.
> (b) None of the funds provided for Processing, analysis, and collaboration tools for counterterrorism foreign intelligence shall be available for deployment or implementation except for:
> (1) lawful military operations of the United States conducted outside the United States; or
> (2) lawful foreign intelligence activities conducted wholly overseas, or wholly against non-United States citizens.

Department of Defense Appropriations Act, Pub. L. No. 108-87, § 8131(a)–(b), 117 Stat. 1054, 1102 (2004). Four research programs of the Information Awareness Office were continued, but none were related to "pattern analysis" or "data mining." *See* H.R. CONF. REP. NO. 108-283, at 327 (2003), *as reprinted in* 2003 U.S.C.C.A.N. 1168, 1189.

[42] *See* Dempsey & Flint, *supra* note 41, at 1464.

[43] *See* John Poindexter, Director, Information Awareness Office of DARPA, Remarks at DARPA Tech 2002 Conference (Aug. 2, 2002), *available at* http://www.fas.org/irp/agency/dod/poindexter.html.

[44] *See, e.g.*, Kathleen M. Sullivan, *Under a Watchful Eye: Incursions on Personal Privacy*, *in* THE WAR ON OUR FREEDOMS 128, 132 (Richard C. Leone & Greg Anrig, Jr., eds., 2003) ("At the extreme [datamining] could be a vehicle for politically motivated spying and intimidation reminiscent of the worst features of the J. Edgar Hoover era."); William Safire, *You Are a Suspect*, N.Y. TIMES, Nov. 14, 2002, at A35 ("[John] Poindexter is now realizing his 20-year dream: getting the 'data-mining' power to snoop on every public and private act of every American . . . . Poindexter's assault on individual privacy rides roughshod over such oversight. He is determined to break down the wall between commercial snooping and secret government intrusion."); American Civil Liberties Union: Q&A on the Pentagon's "Total Information Awareness" Program, http://www.aclu.org/privacy/spying/15578res20030420.html (last visited June 5, 2007) ("[TIA] would kill privacy in America.").

could be effective at all. The "pattern based" search approach dramatically increases the amount of actions that must be watched and, more relevantly, increases the sets of actions that must be watched.[45] Unlike CAPPS II, TIA would have to identify one person's identity across databases without a reliable "starting place," such as the plane ticket purchase which triggers a CAPPS II investigation.[46] While driver's license numbers and social security numbers uniquely identify an individual, they are often not recorded in commercial transactions, such as paying for flight lessons or buying products which could be used in explosives.

[26] The TIA was not merely interested in individuals, but rather patterns of behavior, which could occur among small groups of terrorists working together.[47] For a population of *n* people, the set of all sets of those people is 2^n.[48] Certainly this is astronomically larger than the sets worth watching, but even for a small population, the number of sets worth surveillance is probably going to be larger than the number of atoms in the universe, which is estimated to be between 2^{240} and 2^{320}.[49] Even if we were only watching the activities of sixty-four people, the number of possible sets of those people exceeds the address space of the largest server computers which existed in 2003.[50]

[27] Suppose also that on a particular day there are 10,000 applications for a visa or passport, 10,000 applications for a driver's license, 10,000 airline ticket purchases, and 10,000 purchases of nitrogen fertilizer. If a terrorist were working with partners or using different identities, the program would need to determine if any of the *combinations* of transactions was suspicious. In this case, there are $10{,}000^4$ or

[45] *See e.g.* Dempsy & Flint, *supra* note 41, at 1464 (explaining that pattern-based searches involve searching "large databases when the query does not name a specific individual, address, identification number, or other personally identifiable data element . . . .").
[46] *See id.* at 1466 ("[P]attern-based searches involve queries in the absence of particularized suspicion for data patterns believed to be associated with terrorism.").
[47] Jim Waldo, Analysis of TIA Technology on Privacy (Mar. 17, 2003) (unpublished manuscript, on file with author). The author is very grateful to Dr. Waldo for permitting her to describe his analysis of TIA in this article.
[48] *Id.*
[49] *Id.*
[50] *Id.*

10,000,000,000,000,000 (ten thousand trillion) combinations, assuming (falsely) that only transactions made on the same day are relevant.[51]

[28] The TIA could have been effective if it were only watching the transactions of a few particular individuals under suspicion. But looking only at pre-determined suspicious individuals misses the point of the program — to determine who is suspicious *from* the patterns of behavior.

[29] For those concerned about the costs of perfect law enforcement, the lesson from TIA and CAPPS II is that the wisdom of using technology to enforce laws (or, in this case, to prevent the breaking of laws) is a function not only of the need for the technology but also of the effectiveness. Individuals and tax payers should resist privacy-invading, expensive programs when positive results are non-existent. Similarly, bureaucrats and lawmakers should consider carefully the technological feasibility of a program before implementing it.

B. ACCURACY

[30] A second logistical concern about using technology to catch instances of lawbreaking is that the technology may be inaccurate. Consider red light cameras, which automatically photograph cars entering and speeding through an intersection, usually printing on the photo the date, time, location, speed of the car, and elapsed time between when the light turned red and the car entered the intersection.[52] Sometimes, the cameras have been known to make mistakes.[53] However, red light

[51] *Id*. at 9–10.

[52] For more details on how red light cameras function, see Tom Harris, Howstuffworks "How Red-light Cameras Work," http://auto.howstuffworks.com/red-light-camera.htm/printable (last visited June 7, 2007).

[53] *See, e.g.*, Molly Smithsimon, *Private Lives, Public Spaces: The Surveillance State*, DISSENT, Winter 2003, at 43, *available at* http://dissentmagazine.org/article/?article=534 ("After data were released in San Diego, the court threw out hundreds of traffic tickets. The data showed that accidents at monitored intersections actually increased. The city's vendor company (Lockheed Martin IMS) had shortened the yellow-light time to capture more offenders."); Nicholas J. Garber et al., An Evaluation of Red Light Camera (Photo-Red) Enforcement Programs in Virginia: A Report in Response to a Request by Virginia's Secretary of Transportation 91-93 (Jan. 2005), http://www.thenewspaper.com/rlc/docs/05-vdot.pdf (discussing possible malfunctions of

cameras catch many law violators at intersections that the police simply do not have the manpower to patrol.

[31] A citation from a red light camera produces unease because the average person does not know how to challenge it. If a police officer had seen the driver run a light, the driver could attempt to undermine the officer's account of events. Were you wearing your glasses? When did you see the light change? Did your partner in the squad car notice the light was red as well? The only way to undermine the camera, however, is by determining if it was functioning properly, which might require technological savvy beyond that of the typical driver.

[32] Needing technical expertise or needing to hire an expert witness to challenge a ticket, however, should not be conflated with a lack of confidence in the accuracy of the camera. Indeed, a faulty camera is more likely to be noticed than an officer who typically tickets people who did not actually run lights, because a camera's accuracy can easily be empirically tested. Mere unease with technology, with the strangeness of a machine claiming that a law has been broken, is a poor reason to resist its use.

[33] Whether a technology inaccurately identifies law breaking is important even if mistaken identifications can be corrected in court. This is especially true if false positives place great burdens on individuals wrongly accused. Consider, for example, how the Recording Industry Association of America ("RIAA") uses automated web crawlers to scour the Internet and find material being distributed in violation of federal copyright law.[54] Several times in the past few years, innocent individuals were greatly inconvenienced by mistakes made by the RIAA web crawlers.

---

the cameras and the possibility of false positives) (cited in ZITTRAIN, supra note 9, at 291 n.74).

[54] *See* Declan McCullagh, *RIAA Apologizes for Threatening Letter* (May 12, 2003), http://www.news.com/2100-1025_3-1001095.html (last visited Apr. 10, 2008) [hereinafter McCullagh, Threatening Letter].

[34] In May 2003, the RIAA sent a DMCA notice[55] to Penn State University alleging that one of the astronomy and astrophysics department's FTP sites was unlawfully distributing songs by musician Peter Usher.[56] The site had been flagged because a folder contained the work of a professor emeritus Peter Usher and because the site hosted an mp3 file of an a cappella song performed by astronomers.[57] In the days that followed, the RIAA admitted that it had erroneously sent dozens of copyright infringement notices.[58] In an e-mail sent to CNETNews.com, the RIAA explained that "individuals look at each and every notice we send out. In this particular instance, a temp employee made a mistake and did not follow RIAA's established protocol . . . ."[59] The RIAA also admitted that it does not require its copyright enforcers to listen to allegedly infringing songs.[60]

[35] In a similar incident, the RIAA threatened to sue an innocent woman for sharing copyrighted music. Sarah Ward, a sixty-six year old retired school teacher, was accused of downloading "I'm a Thug" by rapper Trick Daddy, among other songs.[61] A self-described "computer neophyte," Ward's computer could not have downloaded the infringing songs.[62] She only used a Macintosh, which could not run the file-sharing program Kazaa that she was accused of using.[63]

[36] The RIAA sued Ward because Comcast had assigned her the Internet Protocol ("IP") address associated with infringing Kazaa user Heath7.[64] Although it is less clear in this case what caused the error, there are

[55] Under section 512 of the Digital Millennium Copyright Act ("DMCA"), copyright owners such as the RIAA can request Internet service providers remove or disable access to copyrighted material and can subpoena an Internet service provider to discover the name of a copyright infringer using their servers or network. 17 U.S.C. § 512(c)(1)–(3), (h) (2000).
[56] McCullagh, Threatening Letter, *supra* note 54.
[57] *Id.*
[58] McCullagh, Erroneous Letters, *supra* note 4.
[59] McCullagh, Threatening Letter, *supra* note 54.
[60] *Id.*
[61] Chris Gaither, *Recording Industry Withdraws Suit: Mistaken Identity Raises Questions on Legal Strategy*, BOSTON GLOBE, Sept. 24, 2003, at C1.
[62] *Id.*
[63] *Id.*.
[64] *Id.*

several possibilities. Comcast could have matched the wrong name to the IP address provided by the RIAA, or the RIAA could have misidentified the IP address.[65]

[37] The RIAA is understandably reluctant to eliminate web crawlers because they can identify more instances of infringement than can be identified by a team of humans. But, by including a human component to check the findings of the web crawlers (as the RIAA purportedly does), false positives can be limited while maintaining the efficacy of the technology. The human component is critical because of the burdens that incorrect accusations of file-sharing can cause, such as shouldering the cost of hiring defense lawyers or paying a settlement agreement.

C. ABUSE AND UNINTENDED SIDE EFFECTS

[38] Sometimes, even using accurate and effective technology to enforce laws can be harmful due to unintended side effects. Some technologies which aggregate data for ostensibly good uses can later be used to cause harm. Discovering and using personal information to cause harm is nothing new; in 1989, for example, actress Rebecca Schaeffer was shot at her home by a stalker.[66] He had found her by hiring a private investigator to obtain her address from her California Motor Vehicle Record.[67] Schaeffer's death was an unintended and horrific result of a data-gathering program. The government was not abusing its power, yet the existence and accessibility of the information allowed someone else to cause harm.

[39] Information on driver's licenses is not just being kept by Departments of Motor Vehicles anymore. Businesses can also gain access

[65] *Id*.

[66] *See* John T. Cross, *Age Verification in the 21st Century: Swiping Away Your Privacy*, 23 J. MARSHALL J. COMPUTER & INFO. L. 363, 370 (2005).

[67] *See* EPIC DPPA and Driver's License Privacy Page, http://www.epic.org/privacy/drivers/ (last visited June 7, 2007). Following a series of incidents like this, Congress passed the Drivers Privacy Protection Act ("DPPA") to prevent the release of personal information "about any individual obtained by the department in connection with a motor vehicle record . . ." although the statute includes exceptions for disclosures "[f]or use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection[,]" which is precisely how Schaeffer's stalker acquired her address. 18 U.S.C. § 2721(a)(1), (b)(8) (2000).

to the information. Increasingly, states are issuing drivers licenses with a magnetic strip or barcode which can be scanned.[68] Some states encrypt some of the data included on the licenses so they can only be used for law enforcement purposes, but others do not.[69] The included data can be basic, such as a name, address, and license expiration date, or can be more personal and distinctive, such as a social security number, electronic fingerprint or signature image.[70] Although many businesses scan driver's licenses to prevent underage patrons from purchasing tobacco or alcohol, only a few states regulate what can be recorded or when licenses can be swiped. In Texas, a business may not keep information obtained from a scan in a database unless required to do so by the Texas alcohol commission.[71] New Hampshire entirely prohibits the swiping of licenses to verify age.[72] In Ohio, a business may store only a name, date of birth,

[68] Cross, *supra* note 66, at 363-64. The current swipe-able state of driver's licenses is a far cry from the past, when many licenses did not even include pictures. However, the use of driver's licenses as positive identification instead of as mere licenses to drive a motor vehicle was lost some time ago. In one particularly memorable anecdote, after vetoing a bill to put photos on driver's licenses twice, Tennessee Governor Lamar Alexander visited the White House. When the guard asked him for a photo identification, he replied, "We don't have them in Tennessee. I vetoed them." The guard said, "You can't get in without one.'" Alexander was finally admitted when the Governor of Georgia, who did have his photo on his driver's license, vouched for Alexander's identity. Lamar Alexander, *Much as I Hate It, We Need a National ID*, WASH. POST, Mar. 30, 2005, at A15.

[69] Positive Access FAQs, http://www.positiveaccess.com/html/faqs.html (last visited June 7, 2007):

> Some states and provinces have encrypted the ID data on their licenses for various reasons of law enforcement control and/or individual privacy protection. In several cases, these state's [sic] with encrypted data have released information to [legitimate scanning organizations]. . . . [I]n [ ] other instances, the states maintain a strict policy of limiting the release of encryption codes to law enforcement agencies.

[70] *See* Swipe, http://www.we-swipe.us/research.html#info (last visited June 7, 2007).

[71] TEX. ALCO. BEV. CODE ANN. § 109.61(a)–(b) (Vernon 2004); *see also* Cross, *supra* note 66, at 372–73 (discussing the statute in greater depth).

[72] N.H. REV. STAT. ANN. § 263:12(X) (2003) ("It shall be a misdemeanor for any person to: (X) Knowingly scan, record, retain, or store in any electronic form or format, personal information, as defined in RSA 260:14, obtained from any license, unless authorized by the department."); *see also* Cross, *supra* note 66, at 373–74 (discussing the statute in greater depth).

license expiration date, and license number.[73] Similarly, Connecticut only permits businesses to record patrons' names, birthdates, license expiration dates, and identification numbers.[74] Other states apparently encourage the use of license scanning devices. West Virginia, for instance, allows a business to use the performance of a scan as an affirmative defense to charges of selling alcohol or tobacco to a minor.[75]

[40] As so few states regulate the scanning of licenses by private businesses, this use of technology to perfectly enforce the underage drinking and tobacco use laws may have some significant unintended side effects, such as violent crime.[76] Many businesses automatically store whatever information their scanners can decode.[77] Scanner manufacturers allow businesses to store scanned information in a local on-site database.[78] A bar employee fairly easily could make a list of all customers' home addresses who were of a certain age and physical type.[79] It would be easy

---

[73] OHIO REV. CODE ANN. § 2927.021(D)(1) (LexisNexis 2003); OHIO REV. CODE ANN. § 4301.61(D)(1) (LexisNexis 2003); *see also* Cross, *supra* note 66, at 374–78 (discussing the statute in greater depth).

[74] CONN. GEN. STAT. § 30-86(d)(1) (2003):

> No permittee or permittee's agent or employee shall electronically or mechanically record or maintain any information derived from a transaction scan, except the following: (A) The name and date of birth of the person listed on the driver's license or identity card presented by a cardholder; (B) the expiration date and identification number of the driver's license or identity card resented by a cardholder;

CONN. GEN. STAT. § 53-344(e)(1) (2003):

> No seller or seller's agent or employee shall electronically or mechanically record or maintain any information derived from a transaction scan, except the following: (A) The name and date of birth of the person listed on the driver's license or identity card presented by a cardholder; (B) the expiration date and identification number of the driver's license or identity card presented by a cardholder;

see also Cross, *supra* note 66, at 378–79 (discussing the statute in greater depth).

[75] W. VA. CODE § 60-3A-25a (2004); *see also* Cross, *supra* note 66, at 381 (discussing the statute in greater depth).

[76] Cross, *supra* note 66, at 392.

[77] *Id.*

[78] Lee, *supra* note 2 ("[W]ith Intelli-Check's scanners and those of many other manufacturers, the information is stored locally, with the client gaining easy access.").

[79] *See* Kim Zetter, *Great Taste, Less Privacy*, WIRED, Feb. 6, 2004, *available at* http://www.wired.com/politics/security/news/2004/02/62182.

to take advantage of the available information and use it towards malicious ends.

[41] Data-gathering by well-intentioned governments can also lay the groundwork for abuse by future governments. In Nazi Germany, South Africa, and Rwanda, information about religion, ethnicity and tribal affiliation, which was originally gathered with more innocent intentions, was later used to facilitate genocide and apartheid.[80] In Rwanda, race was included on the national identification card a full sixty years before it became a tool of genocide.[81] Even if the government always remains a good actor, the use of scanning devices could still allow vast quantities of information about individuals to be stored and aggregated by private individuals. There are no guarantees about what the future holds, so governments and businesses should check themselves and their future selves by avoiding unnecessary data collection.

[42] For those who believe alcohol and tobacco should be kept away from minors, eliminating card swiping to prevent underage consumption would be unfortunate. However, there are options which can minimize both abuse and lawbreaking. As Eugene Volokh succinctly postulated, "it's important that the potential for abuse is limited and limitable. . . . Instead of denying potentially useful tools to the police, we should think about what control mechanisms we can set up to make abuse less likely."[82] In this case, states could take greater measures to regulate what can be done with scanned data and what can be stored. Perhaps disallowing any information storage strikes the ideal balance, minimizing both underage alcohol and tobacco use and the potential for abuse.

[43] Generally speaking, whether a technology should be used depends on how easily abuse can be limited. In the case of scanning licenses, increased regulation may be enough to prevent significantly dangerous abuse; if no information is saved from a scan, the potential for abuse is greatly diminished and much abuse simply cannot happen. However, the

[80] Testimony of Jim Harper, Director of Information Policy Studies, Cato Institute, to the Senate Committee on the Judiciary, Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns (May 8, 2007), *available at* http://www.cato.org/testimony/ct-jh20070508.html.
[81] *Id*.
[82] Volokh, *supra* note 8.

use of racial information on the Rwandan national identification cards to facilitate genocide raises an additional concern. Volokh notes that

> in a legal and political system that relies heavily on precedent and analogy, the slippery slope is a real risk. . . . [For example,] once the government invests money in [traffic] cameras, voters might want to get the most law-enforcement bang for the buck by having the police store, merge, and analyze the gathered data. This slippage isn't certain, but it's not implausible.[83]

Lawmakers and citizens must also be alert enough to curtail programs where the potential for future abuse cannot be eliminated, even if the immediate results are positive.

V. LEGAL CONCERNS

[44] A second set of concerns which arises when considering the wisdom of perfect law enforcement are legal in nature. Even when law enforcing technologies are effective, accurate, and abuse-proof, they may still be in tension with the constitution or other important legal doctrines.

A. THE FIRST AMENDMENT AND PRIOR RESTRAINT

[45] Many software programs are being designed to prevent copyright infringement. In cases of performance or copying of media, another term for "prevention" could be "prior restraint of expression." Courts generally presume that restraining speech before it is uttered violates the First Amendment, even when the speaker can be punished for the speech after it is made.[84] Of course, the First Amendment functions differently on copyrighted works. Under the First Amendment, the government may not prevent you from publishing a pamphlet, but under the Copyright Act, the government may be employed to prevent others from publishing copies of

[83] *Id*.
[84] *See* New York Times Co. v. United States, 403 U.S. 713, 722–23 (1971).

your pamphlet.[85] Similarly, if you place a copyrighted music video on youtube.com and claim that the video expresses your feelings much better than you could using your own words, the video would undoubtedly be *speech*.[86] But you would also undoubtedly be liable for copying the video.

[46] Courts have historically been quick to dismiss First Amendment claims in copyright suits.[87] Perhaps the most popular and legally successful view of the relationship between the First Amendment and copyright is that of Robert Denicola and Melville Nimmer,[88] who believe that fair use,[89] and the idea/expression distinction,[90] provide enough limits

---

[85] *See* Rebecca Tushnet, *Copyright as a Model for Free Speech Law: What Copyright Has in Common With Anti-Pornography Laws, Campaign Finance Reform, and Telecommunications Regulation*, 42 B.C. L. REV. 1, 2 (2000).

[86] This example was originally given by Mark Tushnet in his Free Speech class, Dec. 5, 2006.

[87] Tushnet, *supra* note 85, at 6; *see also, e.g.*, Walt Disney Prods., v. Air Pirates, 581 F.2d 751, 758 (9th Cir. 1978) ("[D]efendant's [First Amendment] claim can be dismissed without a lengthy discussion . . . ."); *NII Copyright Protection Act of 1995: Joint Hearing on H.R. 2441 and S. 1284 Before the Subcomm. on Courts and Intellectual Property of the House Judiciary Comm. and the Senate Judiciary Comm.*, 104th Cong. (1995) (statement of Bruce Lehman, Commissioner of Patents):

> The First Amendment has always provided a completely different standard with aregard to liability for actions that constitute speech as compared to actions that constitute copyright infringement. They're really just apples and oranges. . . . [I]t really does a disservice to both areas of law . . . to analogize from one to the other.

[88] *See* Tushnet, *supra* note 85, at 6.

[89] "[T]he fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright." 17 U.S.C. § 107 (2000).

[90]

> Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression . . . . In no case does copyright protection for an original work of authorship extend to any idea . . . regardless of the form in which it is described, explained, illustrated, or embodied in such work.

17 U.S.C. § 102 (2000); *see* Baker v. Selden, 101 U.S. 99, 100–101 (1879) ("Where the truths of a science or the methods of an art are the common property of the whole world, any author has the right to express the one, or explain and use the other, in his own way.").

on copyright to satisfy any concerns about free speech.[91] Alternative views include, for example, Rebecca Tushnet's belief that some aspects of copyright law may unnecessarily and unconstitutionally infringe on First Amendment interests.[92]

[47] Although First Amendment issues rarely play a role in copyright disputes, the disfavoring of prior restraints of expression in First Amendment jurisprudence may still be relevant to perfect prevention of copying. Even in copyright cases, courts have been reluctant to allow copyright holders to prevent an expression from reaching an audience. In *Stewart v. Abend*, for instance, Abend established he owned the renewal rights in the copyrighted short story "It Had to Be Murder" and, by extension, rights in the story's derivative work, the movie *Rear Window*.[93] Abend had sought an injunction against the ongoing distribution of the movie, presumably so he could negotiate a very favorable royalty agreement, but the Ninth Circuit ruled in *Abend v. MCA, Inc.* that damages, fixed by the district court, should be awarded to him for the continued distribution of the film.[94] The remedy, which was in essence a forced license, displays the court's reluctance to allow someone the power to prevent speech — where in this case, the speech was a film of significant value.

[48] Saying that the Ninth Circuit's decision in *Abend v. MCA, Inc.* demonstrates an implicit repudiation of prior restraint in copyright law would be a drastic overstatement. The makers of *Rear Window* had properly acquired the rights to make the film; the question of whether Abend could enjoin the dissemination of the film only arose because Cornell Woolrich, the author of "It Had to Be Murder," died before the copyright renewal period for the story had concluded.[95] Dying without a surviving spouse or child, the copyright reverted to a trust administered by

[91] *See* Tushnet, *supra* note 85, at 6; *see also* Robert C. Denicola, *Copyright and Free Speech: Constitutional Limitations on the Protection of Expression*, 67 CAL. L. REV. 283, 289–99 (1979); Melville B. Nimmer, *Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?*, 17 UCLA L. REV. 1180, 1190 (1970).
[92] *See* Tushnet, *supra* note 85, at 6, 27–30.
[93] Stewart v. Abend, 495 U.S. 207, 226- 27 (1990).
[94] Abend v. MCA, 863 F.2d 1465, 1479–80 (9th Cir. 1988).
[95] *Id.* at 1467.

Woolrich's executor, who sold it to Abend.[96] Thus, the court's decision may have been motivated by the sense that the complications of copyright renewals and reversions should not result in derivative works being held hostage—perhaps especially not by individuals like Abend, who had no relation to the creator of the original work. Nonetheless, *Stewart v. Abend* demonstrates that there is some aversion to prior restraint in copyright, perhaps one that could only grow to have teeth if significant copyright reforms pass.

[49] Although the First Amendment does not currently protect against perfect prevention of copying, the philosophy behind the prior restraint doctrine may still be reason to eliminate the wide use of digital rights management systems. Historically, many have argued that the certainty of punishment in violating a prior restraint will have a greater "chilling effect" on speech than post-speech criminal sanctions.[97] Stephen Barnett argued for the validity of the prior restraint doctrine because the "collateral bar" rule prevents a speaker from challenging the constitutional validity of an injunction on speech after the injunction has been disobeyed.[98]

---

[96] *Id.*

[97] ALEXANDER M. BICKEL, THE MORALITY OF CONSENT 61 (1975).

> Prior restraints fall on speech with a brutality and a finality all their own. Even if they are ultimately lifted they cause irremediable loss — a loss in the immediacy, the impact, of speech. They differ from the imposition of criminal liability in significant procedural respects as well, which in turn have their substantive consequences. The violator of a prior restraint may be assured of being held in contempt; the violator of a statute punishing speech criminally knows that he will go before a jury, and may be willing to take his chance, counting on a possible acquittal. A prior restraint, therefore, stops speech more effectively. A criminal statute chills, prior restraint freezes. Indeed it is the hypothesis of the First Amendment that injury is inflicted on our society when we stifle the immediacy of speech.

Id.

[98] Stephen R. Barnett, *The Puzzle of Prior Restraint*, 29 STAN. L. REV. 539, 551–53 (1977).

> By virtue of [the collateral bar] rule, a newspaper or broadcast station subject to a gag order is placed in a trilemma of chilling effects unique to a prior restraint situation. It can comply with the order and take no legal steps, thereby accepting the suppression. It can appeal the order directly, but it must obey the interim restraint while it does so . . . . Or it

[50] The "chilling effect" theory can be criticized if one believes that injunctions will not restrain speech significantly more than criminal sanctions. But in the context of copyright law, the use of digital rights management systems has a chilling effect by its very nature. A copyright holder employs DRM to prevent the copying of its work and to prevent the dissemination of speech by preventing it from being uttered.[99] The use of DRM creates the opposite result of *Stewart v. Abend*. Abend was paid damages for each instance of copyright infringement that occurred when copies of *Rear Window* were sold or shown, but he could not prevent it from being disseminated.[100] On the other hand, DRM prevents copyright infringing speech in the first instance.[101] A potential copyright infringer would not suffer the consequences of his actions by paying damages or going to jail, but would be unable to infringe a copyright at all.[102]

[51] Why might this be problematic? Could one not see DRM as saving the court system and copyright owners a lot of time and money that would have been spent trying to punish copyright infringers? A potential problem can be analogized from a traditional First Amendment scenario. Consider a situation similar to *New York Times Co. v. United States*, where a reporter has a government secret in his possession that he would be punished for publishing.[103] In our hypothetical system of perfect prevention, the reporter would not be able to publish the material at all. However, without perfect prevention, the reporter has a choice: do nothing and avoid punishment, or publish the secret and be sanctioned. The reporter has to weigh, in effect, what the secret is worth to the public against the value of his own freedom or finances. People being the self-interested beings that they are, one would expect this heuristic balancing

> can publish in the face of the gag order, but only at the price of forfeiting its legal and constitutional objections to the order and thus, in all probability, embracing a contempt conviction.

Id. at 553.

[99] *See* Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49, 60 (2006).

[100] Abend v. MCA, 863 F.2d 1465, 1480 (9th Cir. 1988).

[101] *See* Armstrong, *supra* note 99, at 60.

[102] *See id.*

[103] New York Times Co. v. United States, 403 U.S. 713 (1971).

to result in secrets important to the public good being revealed and secrets that are merely titillating or prurient being held back.[104]

[52] In the copyright context, the reporter is replaced with an aspiring copyright infringer—a character for whom one typically has less esteem but whose role may be similarly important. The aspiring infringer does not trade in secrets and rhetoric but in culture, most of which is legally available for a fee. The aspiring infringer performs a similar balancing test as the reporter, asking if the value of the infringement (both to the public and to the infringer) is outweighed by the cost of being caught. However, unlike in the government secret scenario, fewer would be willing to accept this balancing test as justified, primarily because it is so difficult to think of how a copyright infringement could be vitally important to society.

[53] However, there are and have been situations when perfect prevention of infringement might have been unfortunate. Consider, for example, the infamous *Star Wars Holiday Special*[105] and the critically-acclaimed *Grey Album*.[106]

[54] *The Star Wars Holiday Special* was a two-hour television special broadcast in its entirety in the United States only once on Friday,

---

[104] This argument is similar to the equilibrium argument proposed in Bickel's *A Morality of Consent*. Bickel argued that, while the government is entitled to keep things private, the government's power would be frightening if it were not offset by the power of the press. The value of the government's privacy and the public discourse are irreconcilable, and so a balance is struck by the struggle. BICKEL, *supra* note 97, at 79–82. *But see* Cass Sunstein, *Government Control of Information*, 74 CAL. L. REV. 889, 901–02, 904 (1986):

> [Bickel's] equilibrium theory is vulnerable because it does not address.
> . .
> . . . .
> the actual incentives of the press and government; the respective power of the countervailing forces; and what the proper baseline for evaluating outcomes should be…[The] equilibrium theory [is] impressionistic and relies on premises that are both unsupported and unlikely.

[105] For more information, see Star Wars Holiday Special, http://www.starwarsholidayspecial.com (last visited Oct. 15, 2007).

[106] *See* DJ Dangermouse – The Grey Album Download, http://www.illegal-art.org/audio/grey.html (last visited Oct. 15, 2007).

November 17, 1978.[107] David Hofstede, author of *What Were They Thinking?: The 100 Dumbest Events in Television History*, ranked the holiday special at number one and called it "the worst two hours of television ever."[108] It is rumored that *Star Wars* creator George Lucas once said: "[i]f I had the time and a hammer, I would track down every copy of that program and smash it."[109] Unfortunately for George Lucas, the special has achieved a cult status because VHS and Betamax recordings of the broadcast have been copied.[110]

[55] *The Grey Album*, on the other hand, was a "critically praised"[111] collection arranged by Brian Burton (better known as D.J. Dangermouse) which mixed tracks from Jay-Z's *The Black Album* and the Beatles' *White Album*.[112] Burton complied with notice by White Album rights holder EMI to cease and desist distribution of the album, but Burton's fans were not so conciliatory.[113] They staged "Grey Tuesday," during which more than 150 sites offered the album for download.[114] While Burton theoretically could have purchased a license from EMI to use the *White*

---

[107] L. Wayne Hicks, *When the Force Was a Farce*, http://www.tvparty.com/70starwars.html (last visited Mar. 31, 2008).

[108] DAVID HOFSTEDE, WHAT WERE THEY THINKING?: THE 100 DUMBEST EVENTS IN TELEVISION HISTORY 204 (2004).

[109] *See* L. Wayne Hicks, *When the Force Was a Farce*, http://www.tvparty.com/70starwars.html (last visited Mar. 31, 2008).

[110] *See, e.g.*, Star Wars Holiday Special, http://www.starwarsholidayspecial.com (last visited June 12, 2007):

> This site was created as a labor of love in homage to the 25th anniversary of The Star Wars Holiday Special, which aired one time only on November 17th, 1978 and has been virtually lost ever since. The intent was to gather as much as there is to possibly know about the Holiday Special and document it in great detail, since this has never really been done before.

Star Wars Holiday Special!, http://www.i-mockery.com/minimocks/starwars-holiday (last visited June 12, 2007); Stomp Tokyo Video Reviews — Star Wars Holiday Special, http://www.stomptokyo.com/movies/star-wars-holiday-special.html (last visited June 12, 2007).

[111] *See, e.g.*, Dangermouse News, http://www.dangermousesite.com/news_weekly_best.html (last visited Oct. 15, 2007) (highlighting the Grey Album's praise from *Entertainment Weekly*).

[112] Bill Werde, *Defiant Downloads Rise from Underground*, N.Y. TIMES, Feb. 25, 2004 at E3.

[113] *Id.*

[114] *Id*.

Album, the Beatles do not typically allow their work to be sampled even for a fee.[115] EMI did not file suit, despite their initial protests against the album.[116]

[56] Both the *Grey Album* and the *Star Wars Holiday Special* are serious examples of an aspiring infringer's dilemma. Is it worth risking a possible lawsuit in order to copy significant pieces of culture which are contraband? In the present world which generally lacks perfect prevention, the *Star Wars Holiday Special* and the *Grey Album* are tolerated. The owners of the special do not want to go through the effort to prevent its dissemination and preservation, most likely because they just do not care enough to do so and because they do not wish to draw any further attention to the show. EMI may have backed down in the face of the widespread disobedience and anger that destroying the *Grey Album* would create. However, in a world of perfect prevention, an infringer could not practice the "civil disobedience" that the *Star Wars Holiday Special* and the *Grey Album* require to persist, and perhaps the world would have significantly less rich speech and cultural landmarks. There would be no uses to tolerate. Potentially valuable pieces of speech or culture such as mash-ups could disappear. Although the law does not currently recognize this concern under the purview of the First Amendment, a belief that speech and media should be preserved and disseminated should still prevent policymakers from facilitating powerful means of perfect prevention.

B. THE FIRST AMENDMENT AND FAIR USE

[57] A more significant First Amendment issue could be raised if courts come to fully accept Denicola and Nimmer's belief that fair use, along with the idea/expression distinction, saves the copyright statute from being unconstitutional on First Amendment grounds.[117] Although fair use is an affirmative defense to copyright infringement,[118] many digital rights

[115] *Id.* ("To create a collection like 'The Grey Album' legally, an artist would first have to get permission to use copyrighted material. . . . Many artists, however, like the Beatles, will not allow their music to be sampled.")
[116] DJ Dangermouse – The Grey Album Download, http://www.illegal-art.org/audio/grey.html (last visited Oct. 15, 2007).
[117] *See* Denicola, *supra* note 91, at 289–99; Nimmer, *supra* note 91, at 1190.
[118] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 599 (1994).

management technologies prevent copying which would be fair use because they prevent all instances of copying. Additional barriers to fair use copying have been erected since the passage of the Digital Millennium Copyright Act ("DMCA"). Section 1201 of the Copyright Act states, "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[119]

[58] Although section 1201 provides some limited exceptions to this rule,[120] it does not include a general exception for fair use. Section 1201 seems to say that, so long as a copyright holder can conceal material behind a "technological measure that effectively controls access"[121] to the copyrighted work, the copyright holder can legally eliminate fair use of that work.

[59] Perfect prevention of arguably fair uses does raise some constitutional concerns. In *Eldred v. Ashcroft*, the Court embraced Denicola and Nimmer's view, stating that although copyrights are not categorically immune from challenges under the First Amendment, copyright law's built-in free speech safeguards, such as fair use and the idea/expression distinction,[122] are adequate to address First Amendment concerns so long as Congress does not alter the "traditional contours of copyright protection . . . ."[123] Other courts have also implied that fair use

[119] 17 U.S.C. § 1201(a)(1)(A) (2000). "To 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner . . . ." 17 U.S.C. § 1201(a)(3)(A). "A technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B).

[120] *See, e.g.*, 17 U.S.C. § 1201(d) ("Exemption for Nonprofit Libraries, Archives, and Educational Institutions."); 17 U.S.C. § 1201(e) ("Law Enforcement, Intelligence, and Other Government Activities."); 17 U.S.C. 1201(f) ("Reverse engineering . . . to achieve interoperability of an independently created computer program with other programs . . . ."); 17 U.S.C. § 1201(g) ("Encryption research."); 17 U.S.C. § 1201(i) ("Protection of Personally Identifying Information.").

[121] 17 U.S.C. § 1201 (1999).

[122] Rebecca Tushnet, *Copy This Essay: How Fair Use Doctrine Harms Free Speech and How Copying Serves It*, 114 YALE L.J. 535, 548 (2004).

[123] Eldred v. Ashcroft, 537 U.S. 186, 221 (2002). For a more in depth discussion of the relationship between copyright, fair use, and the First Amendment after *Eldred*, see Stephen M. McJohn, *Eldred's Aftermath: Tradition, the Copyright Clause, and the*

saves the copyright regime from being a First Amendment violation.[124] Thus, section 1201 runs the risk of being unconstitutional under the First Amendment on the basis that it effectively makes fair use of a work illegal if one must circumvent technology to access it.

[60] Despite *Eldred's* statement that fair use prevents the Copyright Act from violating the First Amendment, other cases postulate that the First Amendment provides very little protection for fair use. In *Universal City Studios, Inc. v. Corley*, [125] for instance, the Second Circuit held that the DMCA,[126] was constitutional even though the law effectively eliminated fair uses when copyrighted content was protected by DRM technologies.[127] Corley was enjoined from posting the DeCSS code on his website, a code which allows a person to circumvent CSS, an encryption code that prevents the unauthorized viewing and copying of DVDs.[128] On appeal to the Second Circuit, Corley argued, among other points, that he should be allowed to post the DeCSS code because the DMCA violated the First Amendment and the Copyright Clause by unduly obstructing the "fair use" of copyrighted materials.[129]

[61] Although the Second Circuit did not fully "explore the extent to which fair use might have constitutional protection, grounded on either the

Constitutionalization of Fair Use, 10 MICH. TELECOMM. & TECH. L. REV. 95 (2003), *available at* http://ssrn.com/abstract=991354.

[124] *See, e.g.*, A & M Records v. Napster, 114 F. Supp. 2d 896, 922 (N.D. Cal. 2000) ("[F]ree speech concerns are protected by and coextensive with the fair use doctrine.") (internal quotation marks omitted), *aff'd in part and rev'd in part*, 239 F.3d 1004 (9th Cir. 2001); L.A. Times v. Free Republic, 54 U.S.P.Q.2d (BNA) 1453, 1472 (C.D. Cal. 2000) (holding that free speech concerns "are subsumed within the fair use Analysis"); *see also* Harper & Row, Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 560 (1985) (noting "the First Amendment protections already embodied in the Copyright Act's distinction between copyrightable expression and uncopyrightable facts and ideas, and the latitude for scholarship and comment traditionally afforded by fair use . . . ."); Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 575 (1994) ("From the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose, '[t]o promote the Progress of Science and useful Arts . . . .'") (omission in original).

[125] Universal Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[126] 17 U.S.C. § 1201 (1998).

[127] *Corley*, 273 F.3d at 458.

[128] *Id.* at 442-43.

[129] *Id*. at 436.

First Amendment or the Copyright Clause . . .”[130] because it was beyond the scope of the lawsuit, the court nonetheless noted in dicta, “[w]e know of no authority for the proposition that fair use, as protected by the Copyright Act, much less the Constitution, guarantees copying by the optimum method or in the identical format of the original.”[131] Thus, while the DMCA and CSS may prevent someone from making a digital copy of a DVD to, for example, make a documentary for a film class, a fair user would be able to “point[] a camera, a camcorder, or a microphone at a monitor as it displays the DVD movie.”[132] In other words, according to the Second Circuit, even if fair use were constitutionally protected, the type or form of the fair use could be severely limited.

[62] Even if fair use were not constitutionally protected at all, its value should lead policymakers to question the wisdom of the DMCA and the use of DRM technologies which prohibit all instances of copying. Preventing fair use copies is similar to a surveillance system which experiences too many false positives. The technology may perfectly catch all law violations, but it catches too much, to the detriment and inconvenience of those in the “false positive” group (fair use copiers) and of all potential and actual fair users. Policymakers must ask if the benefit of perfect enforcement—eliminating media “piracy”[133]—is offset by the cost of preventing fair uses of the media. After *Eldred*, however, there is significant reason to believe passing laws that prevent fair uses could violate the First Amendment.

C. THE NECESSITY DEFENSE

[63] Another concern about perfect prevention is that sometimes it is important to break the law to prevent harm. At times, exceptions to laws are written into statutes explicitly. For example, several statutes making

[130] *Id*. at 458.
[131] *Id*. at 459.
[132] *Id*.
[133] Sonia K. Katyal noted the oddity of using the phrase “piracy,” a word that suggests that copying media is “somehow contemporaneously equivalent to crossing the high seas, invading a ship, stealing its contents,
and threatening life.” Sonia K. Katyal, *Privacy v. Piracy*, 7 YALE J. L. & TECH. 222, 267–69 (2004).

murder a crime include an explicit exception for self-defense.[134] Similarly, the Copyright Act includes an exception for "fair uses" of the copyrighted material.[135] At other times, exceptions are not explicit in a statute, but are nevertheless recognized by potential litigants, such as breaking the speed limit to tear away from danger.

[64] Simply, there are times when it is ethical and imperative to break the law. Amongst ourselves, we may disagree about precisely when these situations arise, but most reasonable people would agree that there are times when the law does not anticipate the bizarre states of affairs that can arise and make lawbreaking necessary. This reality has been woven into our jurisprudence. The Supreme Court has recognized "necessity" as a defense to criminal prosecution in situations where "criminal action was necessary to avoid a harm more serious than that sought to be prevented by the statute defining the offense."[136] This defense probably exists even when no exception is explicitly recognized in a criminal statute.[137] The

---

[134] *See, e.g.*, CAL. PENAL CODE § 197 (Deering 1999).

[135] 17 U.S.C. § 107 (2000).

[136] United States v. Bailey, 444 U.S. 394, 410 (1980) (internal citations omitted). The Ninth Circuit has provided one framework for a necessity defense:

> As a matter of law, a defendant must establish the existence of four elements to be entitled to a necessity defense: (1) that he was faced with a choice of evils and chose the lesser evil; (2) that he acted to prevent imminent harm; (3) that he reasonably anticipated a causal relation between his conduct and the harm to be avoided; and (4) that there were no other legal alternatives to violating the law.

United States v. Aguilar, 883 F.2d 662, 693 (9th Cir. 1989).

[137] *Bailey*, 444 U.S. at 425 (Blackmun, J., dissenting) (having "no difficulty in concluding that Congress intended the defenses of duress and necessity to be available" to prison escape defendant); *id.* at 415 n.11 (Rehnquist, J., majority opinion) (noting that the majority's "principal difference with the dissent, therefore, is not as to the existence of [the necessity] defense but as to the importance of surrender as an element of it."). *But see* United States v. Oakland Cannabis Buyers' Cooperative, 532 U.S. 483, 490 (2001) ("[I]t is an open question whether federal courts ever have authority to recognize a necessity defense not provided by statute."). Three justices concurred in the result of *Oakland Cannabis*, stating that

> the Court gratuitously casts doubt on 'whether necessity can ever be a defense' to *any* federal statute that does not explicitly provide for it, calling such a defense into question by a misleading reference to its existence as an 'open question.' . . . [O]ur precedent has expressed no doubt about the viability of the common-law defense, even in the

rationale for the rule places great faith in individual judgment; as the Ninth Circuit said,

> In some sense, the necessity defense allows us to act as individual legislatures, amending a particular criminal provision or crafting a one-time exception to it, subject to court review, when a real legislature would formally do the same under those circumstances. For example, by allowing prisoners who escape a burning jail to claim the justification of necessity, we assume the lawmaker, confronting this problem, would have allowed for an exception to the law proscribing prison escapes.[138]

[65] In a system of "perfect prevention," technology could remove the ability to break laws in situations where the necessity defense would be applicable. Here, as when we considered prior restraints on speech, preventing a law from being broken has a different effect than punishing a lawbreaker after the fact. In cases where a necessity defense could be used, whether or not an individual can break a law is critical. There is a need to break the law to avoid some greater ill, and so whether the law is broken determines whether the ill was averted. Any technology which prevents law breaking before the fact—for example, one which could prevent cars from exceeding the speed limit—risks creating harm by failing to allow for situations where law breaking is necessary. The use of such technology should be avoided in all cases lacking extremely powerful countervailing factors.

D. THE FOURTH AMENDMENT

[66] Using technology to search computers connected to the Internet has the potential to violate the Fourth Amendment. These issues arise not because of the "perfect" nature of the enforcement, but rather because of

---

> context of federal criminal statutes that do not provide for it in so many words.

Id. at 501 (Stevens, J., concurring) (quoting majority opinion) (citing *Bailey*, 444 U.S. at 415). In the recent Ninth Circuit decision *Raich v. Gonzales*, 500 F.3d 850 (2007), the court stated, "We do not believe that the *Oakland Cannabis* dicta abolishes more than a century of common law necessity jurisprudence."

[138] United States v. Schoon, 971 F.2d 193, 196–97 (9th Cir. 1991).

the types of surveillance technologies which are likely to be used to monitor the activities of web surfers and personal computer users.

[67] Personal computing software and appliances are increasingly "tethered," that is able to relay or receive information from their manufacturers.[139] A TiVo knows whether it frequently watches PBS or Comedy Central and can send this information back to TiVo, Inc.[140] This is how we know that Janet Jackson's "wardrobe malfunction" during the 2004 Super Bowl was replayed three times more than any other moment during the Super Bowl Broadcast.[141] Because many computers are perpetually connected to the Internet, many software programs such as operating systems and antivirus programs are designed to automatically update themselves.[142] Automatic updates change or add code to an individual computer. While most updates are desirable and useful, there is nothing to stop an update from adding code which will search a computer's files and documents or turn on the computer's microphone or camera.[143]

[68] Tethered appliances make it possible for law enforcement and others to perform searches without any obvious intrusion. The police do not have to break down front doors to search through photo albums looking for obscenity; they do not even have to physically place a wiretap outside of a home. If there is software on someone's computer which will do it, law enforcement could search that person's hard drive and send a report on what was found without that person ever being aware of the search.

[69] When, if ever, would such searches raise a Fourth Amendment issue? The answer depends on how the searching software was installed on a

[139] ZITTRAIN, *supra* note 9, at 100–02.
[140] *See id*. at 103-04 (discussing TiVo and similar "tethered" appliances); TiVo Privacy Policy, http://www.tivo.com/5.11.3.asp (last visited Nov. 15, 2007).
[141] Ben Charny, *Jackson's Super Bowl Flash Grabs TiVo Users* (Feb. 2, 2004), http://news.com.com/2100-1041_3-5152141.html (last visited Apr. 10, 2008) (cited in ZITTRAIN, *supra* note 9, at 279 n.38).
[142] *See, e.g.*, Update your Computer Automatically, http://www.microsoft.com/athome/security/update/bulletins/automaticupdates.mspx (last visited June 19, 2007); AVG Anti-Virus and Internet Security, http://www.grisoft.com/ww.why-avg (last visited June 19, 2007) ("High speed automatic updates, certified and by all major independent antivirus certification companies.").
[143] *See* ZITTRAIN, *supra* note 9, at 125.

computer. If the software is installed voluntarily and the user is informed that the information it collects may be shared with government authorities, then the Fourth Amendment is unlikely to be activated because the user consented to the search. If the software provider has a privacy policy that promises not to share found information, the situation also probably will not raise a Fourth Amendment issue. While laws designed to protect privacy may be activated by a private company sharing information about its clients, the Fourth Amendment likely would not be at issue. Fourth Amendment case law indicates there is no constitutional problem with the government acting on information gathered from third parties who came by the information voluntarily.[144] "[T]he law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent . . . ."[145]

[70] A particularly relevant situation implicating the Fourth Amendment in computer searches was discussed by Michael Adler in his note "Cyberspace, General Searches, and Digital Contraband."[146] Adler asked whether there would be a Fourth Amendment issue with what he called a "perfect search," an "automated, wide-scale search that could hypothetically scan through hundreds of millions of files but would report to authorities only the presence of files containing contraband."[147] Such a search would be without consent— the code which allowed the search would have to have been installed without the computer user's knowledge—and would be designed to find digital contraband such as illegally copied media, child pornography, or other obscenity.[148] The search program would ignore other material on the computer, even if it were illegal or scandalous, and would not be tempted to peek at other information as a human investigator would.[149] In other words, although the searches would take place "dragnet-style"—without probable cause or any particular reason to think a given computer contained any contraband—the searches would (in Adler's hypothetical) produce no

[144] *See* United States v. White, 401 U.S. 745 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966).
[145] *White*, 401 U.S. at 752.
[146] Adler, *supra* note 11.
[147] *Id*. at 1093–94.
[148] *Id.* at 1112.
[149] *Id.* at 1098.

false positives, have virtually no impact on property, and be virtually unnoticeable by the computer user.[150]

[71] *Prima facie*, such a search would appear to violate the Fourth Amendment if performed without a warrant. In the seminal Supreme Court decision of *Katz v. United States*, Justice Stewart explained, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, must be constitutionally protected."[151] People generally expect their digital copies of pictures and documents to be as private as those they keep in a file cabinet in their home. After *Katz*, the Fourth Amendment's applicability would appear certain.

[72] Two cases following *Katz* bring this certainty into doubt. In *United States v. Place*, the Court found that a dog sniffing luggage for narcotics did not violate the Fourth Amendment.[152] Because the sniff did not require opening the luggage and exposing non-contraband items, the information revealed was limited to the revelation of contraband and did not constitute a Fourth Amendment search.[153] Some courts initially read the *Place* decision to rest on the fact that odors presumably diffused outside of the bags and thus were publicly accessible.[154] However, the Court emphasized in *United States v. Jacobson* that the decisive fact in *Place* was that "government conduct . . . could reveal nothing about non-contraband items."[155] In *Jacobson*, federal agents tested a sample of white powder which had been accidentally discovered and, while destroying the sample, verified that it was cocaine.[156] The Court explained, "governmental conduct that can reveal whether a substance is [contraband], and no other arguably 'private' fact, compromises no

[150] *Id.* at 1100.
[151] Katz v. United States, 389 U.S. 347, 351–52 (1967) (internal citations omitted).
[152] United States v. Place, 462 U.S. 696, 707 (1983).
[153] *Id.*
[154] *See, e.g.*, United States v. Lewis, 708 F.2d 1078, 1080 (6th Cir. 1983) (holding that the use of a trained dog to detect odors of illegal drugs emanating from luggage and other closed containers was not a Fourth Amendment violation because the odors were accessible to the public).
[155] United States v. Jacobson, 466 U.S. 109, 124 n.24 (1984).
[156] *Id.* at 111-12.

legitimate privacy interest."[157] Thus, police may search for contraband without a warrant so long as the search "could, at most, have only a *de minimus* impact on any protected property interest."[158]

[73] Under *Place* and *Jacobson*, it would seem that a "perfect search" might get a constitutional free pass so long as the proper safeguards against abuse were put in place. However, the Court has recently adopted a more restrictive attitude towards new ways of searching. In *Kyllo v. United States*, the Supreme Court considered whether law enforcement agents could use a thermal imaging device to detect infrared radiation from high-intensity lamps typically used to grow marijuana indoors.[159] The majority held, without addressing *Place* or *Jacobson*, that when "the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[160]

[74] What *Kyllo* means for the constitutionality of the "perfect search" is unclear. The thermal imagers in *Kyllo* were not directly searching for contraband, but rather for legal property—the heat lamps—which is a strong indication of contraband. The search revealed something more than the presence of contraband: it revealed the presence of heat lamps, an arguably private fact. Thermal searches might sidestep the *Jacobson* exception to the warrant requirement without the *Kyllo* decision having an impact on the constitutionality of a "perfect search."

[75] On the other hand, while a theoretically perfect search might be captured by the *Place-Jacobson* exception, even the best written searching programs might reveal more than is constitutionally acceptable under *Place* and *Jacobson*. Consider that any program would have to install itself on the computer it was searching, creating the possibility of interrupting or affecting another program's functioning. Further, the program would have to reveal *nothing* other than the presence of contraband, even private information that is not usually considered

[157] *Id*. at 123.
[158] *Id.* at 125.
[159] Kyllo v. United States, 533 U.S. 27, 30-31 (2001).
[160] *Id.* at 40.

sensitive, such as the operating system a person is using. Any surveillance program that could actually be written might be revealing or risk injuring property (i.e. other computer programs) and thus fall outside the *Place-Jacobson* exception.

[76] The constitutionality of a perfect search, therefore, may depend on the specifics of the search program itself. Yet, the risk of affecting other aspects of a person's computer may be enough to make all such searches unconstitutional under the Fourth Amendment.

VI. PHILOSOPHICAL CONCERNS

[77] Logistical and legal concerns aside, there are numerous philosophical and public policy reasons to resist the use of technology to facilitate law enforcement.

A. LAW ENFORCEMENT IS MEANT TO BE DISCRETIONARY

[78] One of the most significant reasons to oppose perfect enforcement is precisely because it would catch all instances of lawbreaking. Perfect enforcement of existing laws will not create ideal results, as our laws were written and developed to reflect a world where law enforcement was imperfect or discretionary. Furthermore, for a rule to be enforced perfectly using technology, the rule must be expressed concisely to a computer or similar device; there is no room for a concept as complex as fair use. Such simple expressions of rules will almost necessarily be poor expressions of what behavior is actually desirable.

[79] Historically, laws have not been written or developed with perfect enforcement in mind. Private law or civil action requires one party to bring suit against another; as this takes time, money, and effort and is a strain on relationships, many potential suits are never brought. Similarly, prosecutors have virtually unlimited discretion over what particular crimes to prosecute. As a result, people often get away with petty law violations such as trespassing in a park after dark, driving five miles over the speed limit, or committing a noise violation in a residential neighborhood. A person can talk his way out of a speeding ticket if he is speeding to the hospital to see a very ill relative. Even law violations that are considered more serious such as prostitution or drug possession often go unpunished

due to a lack of resources in the legal system; a prosecutor simply does not have the means and time to try to prosecute every case.

[80] Imperfect application of the law occurs not only because of choice or lack of means to enforce. A law cannot be written to perfectly reflect the goals of its author or authors. This idea has been explored by Frederick Schauer. He explained that most prescriptive rules such as laws are "probabilistic generalizations."[161] That is to say, most rules are created because following them probabilistically effects some goal. Consider the hypothetical rules "no dogs allowed," "speed limit 55," "no one under the age of 21 shall consume alcohol" or "thou shalt not kill."[162] All of these rules exist because of some justification—that parks and restaurants should be clean and quiet, that people should be safe on the roads, that irresponsible individuals should not drink, that people should live.

[81] Probabilistically speaking, following the rules effects these outcomes. Not permitting dogs in a park will usually make a park quieter and cleaner; driving under fifty-five miles per hour is generally safe; creating a minimum drinking age generally diminishes irresponsible drinking; preventing murder keeps people alive. A rule's factual predicate bears a probabilistic relationship to the concerns of the rule, but in particular cases the connection between the justification and the consequence is absent.[163] Indeed, rules are almost always both over and under inclusive.[164] For example, when the roads are slippery, it may be dangerous to drive at fifty or even forty miles per hour.[165] When many cars are all driving slightly above the speed limit, it may be dangerous to drive below the speed limit.[166] Many under twenty-one can drink responsibly, and many individuals *over* the age of twenty-one cannot.[167] Certainly, in many cases, lawmakers recognize that rules are over and under inclusive, but opt for rules instead of standards because they are easier to apply. Lawmakers know that when they are preventing twenty year olds from drinking, they are preventing some responsible twenty year

[161] FREDERICK SCHAUER, PLAYING BY THE RULES 32 (1991).
[162] *Id*.
[163] *Id*.
[164] *Id.*
[165] *See id.*
[166] *See id.*
[167] *Id.*

olds from imbibing and allowing some irresponsible thirty year olds to cause a ruckus in the local bar. Nonetheless, the rule "you must be twenty-one to drink" is much easier to apply and administer than a system which requires an individualized assessment of everyone's maturity. Rules also make it easier for individuals to understand what the law requires; for example, an individual can much more easily judge if he is driving over fifty-five miles per hour than he can judge if he is driving "safely."

[82] For these reasons, rules are enforced even though we acknowledge they sometimes reach those they should not. Even so, there are still exceptional circumstances that are not written into law but which the legal system is often willing to accept as an excuse for breaking a rule. Consider H. L. A. Hart's famous example of a rule that forbids one to take a vehicle into a public park.[168] Lon Fuller argued that forbidding a statue of a vehicle in the park—say, an old tank on a pedestal placed to commemorate a war—was inconsistent with any sensible purpose behind the "no vehicles in the park" rule.[169] Ignoring the jurisprudential questions of what a judge should do if actually faced with the question of whether the tank should be allowed in the park, one can safely note that it is very unlikely anyone would even try to enforce the "no vehicles in the park" law against whomever was trying to erect the statue, in part because in this case the connection between the consequence of erecting the statute and the justification behind the rule (noisy motors or dangerous machines in the park are unpleasant) is wholly lacking.

[83] These kinds of law violations which no one complains about are very common in copyright law. Violators who photocopy their favorite poems or stories are not hunted down. Sometimes, copyright violations are allowed to continue unimpeded because the copyright infringer has a plausible "fair-use" defense to the infringement.[170] Even though a fair use defense may not succeed, the likelihood that it will may be enough to

[168] H. L. A. Hart, *Positivism and the Separation of Law and Morals*, 71 HARV. L. REV. 593, 607 (1958) (cited in SCHAUER, *supra* note 161, at 212).
[169] Lon Fuller, *Positivism and Fidelity to Law: A Reply to Professor Hart*, 71 HARV. L. REV. 630, 663 (1958).
[170] Daniel D. Hill, Note, *A & M Records, Inc. v. Napster, Inc.: A Victory in the War to Sound the Digital Death Knell for Peer-to-Peer Online File Sharing*, 12 WIDENER L.J. 161, 163-67 (2003).

make a copyright holder unwilling to go through the effort of bringing suit. Sometimes, copyright violations that are clearly illegal but which generate publicity are ignored by copyright holders as well—what Tim Wu calls "tolerated uses."[171] Wu notes that "[t]he industry is deeply conflicted about mild forms of piracy — trapped somewhere between its pathological hatred of 'pirates' and its lust for the buzz piracy can build."[172] Tolerating these infringements is, essentially, utility maximizing. Those who infringe are let off the hook, and content providers get more notice.

[84] Enforcing laws perfectly eliminates this discretion. Software which prevents copyright infringement prevents not only fair uses of copyrighted material but also utility-maximizing illegal uses which might have been tolerated. Further, as commentators have snidely observed, "[u]nless DRM [Digital Rights Management] systems include a 'judge on a chip,' they will remain incapable of determining whether a user is copying part of a work for purposes of piracy or parody."[173] Until recently, a copyright owner had to affirmatively act to punish a copyright violation. Now, using DRM, copyright owners can prevent many more violations. The problem with perfect enforcement is that, figuratively speaking, it prevents or punishes the placement of a tank statue in a park. Not only are fair and tolerated uses curtailed, not only does the woman speeding to the hospital get a ticket, but violations of the law that are clearly justified but which we cannot anticipate are prevented or punished.

B. THE INHERENT VALUE OF PRIVACY

[85] Among the most difficult to articulate aversions to perfect law enforcement is the sense that enforcement methods violate privacy. Lillian BeVier wrote, "[p]rivacy is a chameleon-like word, used denotatively to designate a wide range of wildly disparate interests—from confidentiality of personal information to reproductive autonomy—and connotatively to generate goodwill on behalf of whatever interest is being

[171] Tim Wu, *Does YouTube Really Have Legal Problems?*, SLATE, Oct. 26, 2006, http://www.slate.com/toolbar.aspx?action=print&id=2152264 (last visited Apr. 10, 2008).
[172] *Id.*
[173] C.J. Alice Chen & Aaron Burnstein, *Forward to Symposium: The Law and Technology of Digital Rights Management*, 18 BERKELEY TECH. L.J. 487, 491 (2003).

asserted in its name."[174] Several commentators, notably William L. Prosser[175] and more recently, David J. Solove,[176] have attempted to give the concept a more rigorous definition by providing a taxonomy of the various interests the word "privacy" can denote. The instantiation of privacy invasion which perfect enforcement implicates is that which Prosser called "intrusion upon [one's] seclusion or solitude, or into his private affairs"[177] and what Solove identified as "surveillance"[178] and "intrusion."[179] Intrusion differs from surveillance in that it need not involve the gathering of information; rather, the harm of intrusion is its interference with solitude, or one's ability to retreat from the presence of others.[180]

[86] With these types of privacy invasions in mind, one can ask if there is an inherent value in privacy—freedom from surveillance and intrusion, even if one has nothing to hide, even nothing to be embarrassed about—which could be threatened by various technologies. Certainly, being stared at for extended periods of time can be "invasive and penetrating and also disturbing, frightening, and disruptive."[181] But these feelings of discomfort lack substance; they do not seem strong when compared to arguments that cameras decrease crime and traffic accidents and that searches of computer files are necessary to discover and destroy child pornography rings. If one has nothing to fear from surveillance, can an interest in privacy ever trump a legitimate policy interest in preventing crime and injury?

---

[174] Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL RTS. J. 455, 458 (1995).
[175] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).
[176] David J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).
[177] Prosser, *supra* note 175, at 389. Prosser outlined four kinds of privacy interests that tort law had recognized, specifically: 1. intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; 2. public disclosure of embarrassing private facts about the plaintiff; 3. publicity which places the plaintiff in a false light in the public eye; [and] 4. appropriation, for the defendant's advantage, of the plaintiff's name or likeness. *Id*.
[178] *See* Solove, *supra* note 176, at 491–99.
[179] *See id*. at 552–57.
[180] *Id.* at 552-53.
[181] *Id*. at 553.

[87] Philosopher Thomas Nagel has made progress in giving substance to these kinds of privacy interests, specifically arguing that it is necessary for individuals to have privacy in order to maintain both a public and private identity. According to Nagel, what we seek when we seek privacy is concealment, and "[c]oncealment includes not only secrecy and deception, but also reticence and nonacknowledgment."[182] Reticence and nonacknowledgment are not dishonest. Often, all know the concealed truth. Rather, reticence and nonacknowledgment maintain social order, comfort and respect, and avoid conflict.[183] Nagel offered the example of two individuals, A and B, at a cocktail party.[184] A recently published a terrible review of B's book.[185] Neither of them acknowledges this; rather they talk stiffly about politics and real estate.[186] But, consider the alternative, A announcing, "You conceited fraud, I handled you with kid gloves in that review; if I'd said what I really thought it would have been unprintable; the book made me want to throw up — and it's by far your best."[187] B knows that A thinks this, but would rather be spared the experience of being faced with the cruel comments.[188]

[88] Similarly, consider two friends or public figures who are known for being emotional and who are going through a bitter divorce. Everyone may know that they have had vitriolic arguments and said hateful things; perhaps the two individuals have acknowledged that this is the case. But, having others read the transcript or hear a recording of these arguments, even if they are precisely as imagined, is degrading and uncomfortable for the two arguers. It is the exposure itself which causes a concrete injury, even if what is exposed is not a secret.

[89] Reticence and nonacknowledgment are thus useful, but they are exercised at a cost. The book reviewer is very conscientious about not saying what he thinks; the divorcees refrain from sharing their thoughts with most people they encounter each day. And, just as one needs to

[182] THOMAS NAGEL, CONCEALMENT AND EXPOSURE: AND OTHER ESSAYS 3, 4 (Oxford University Press 2002).
[183] *Id.* at 9-10.
[184] *Id.* at 11.
[185] *Id.*
[186] *Id.*
[187] *Id.*
[188] *Id.*

physically relax after standing all day, these individuals must also relax by turning off their performance in private or with confidants.

[90] Surveillance pressures one to exercise reticence and nonacknowlegment more often, creating tension between the need to put forth a polite and socially acceptable persona and the need to act without consideration for social norms in private. Knowing that someone has filmed one driving, is scanning one's computer files, or is keeping tabs on what television one watches has subtle effects on a person's actions. One may hesitate to rock out to Britney Spears in the car or to TiVo terrible soap operas while at work. The fear that someone else has seen a silly, personal moment or habit, even if no concrete harm can come of the exposure, is chilling. Thus, as Julie Cohen notes, surveillance "threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it."[189] This may well be true, but one is right to ask if the mere dampening of eccentricities is enough to limit measures which could end excessively harmful child pornography, deadly traffic accidents, and even terrorist plotting. Nagel argues,

> The public gaze is inhibiting because, except for infants and psychopaths, it brings into effect expressive constraints and requirements of self-presentation that are strongly incompatible with the natural expression of strong or intimate feeling. And it presents us with a demand to justify ourselves before others that we cannot meet for those things that we cannot put a good face on. The management of one's inner life and one's private demons is a personal task and should not be made to answer to standards broader than necessary.[190]

In essence, Nagel argues that without privacy in which to deal with socially inappropriate inclinations or strong emotions, we would lose our ability to function appropriately (i.e. to exercise nonacknowledgment and reticence) in public and cause social breakdown.

---

[189] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000).
[190] NAGEL, *supra* note 182, at 17–18.

[91] To those concerned with privacy and discretion, Cohen and Nagel's worries seem justified. For others, the effects they warn of sound alarmist. Since the first season of *Survivor* on CBS, reality television has gained such popularity that thousands clamor to be featured on programs that openly seek to embarrass and expose raw emotions and loud, petty conflicts. Britain's closed circuit television ("CCTV") network of over four million public surveillance cameras is widely perceived as "a friendly eye in the sky, not Big Brother but a kindly and watchful uncle or aunt."[191] Even Nagel acknowledges that "what is hidden and what is not may be arbitrary."[192] Indeed, the nature of publicly acceptable behavior has changed over centuries and differs across cultures. The current popularity of blogs and reality television and the non-reaction to Britain's CCTV system indicates that the degree of privacy one needs may be somewhat elastic.

[92] Nonetheless, the writers of blogs and the cast of reality series are volunteers, and British citizens being monitored by CCTV are already subjected to the human public's gaze. More importantly, computers and cameras eventually turn off, and the British pedestrian eventually returns to the privacy of her own home. These individuals still maintain privacy because they, like everyone else, need it in some degree. Nagel argues, "we need privacy to be allowed to conduct ourselves in extremis in a way that serves purely individual demands, the demands of strong personal emotion."[193] And he is correct. Most people would go mad if the paparazzi followed them around and eavesdropped on their every conversation or if video cameras were placed inside every person's home. But if the human need for privacy is somewhat elastic, the risk of harm in other cases may be harder to assess. Does Nagel's argument also undermine the rationales for traffic cameras or computer document searches?

[93] As computers become more deeply woven into people's lives, the notion of searching computer files seems only marginally less invasive than sticking a camera in someone's home. Increasingly, pictures, diaries, and financial information are being stored electronically. Individuals'

[191] JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 36 (2004).
[192] NAGEL, *supra* note 182, at 16.
[193] *Id*. at 17.

private selves are often as much embodied in their personal computers as in their file cabinets and leather-bound journals, and so Nagel's argument is about as persuasive for computer searches as it is for in-home cameras.

[94] Whether the presence of public cameras is an unjustified privacy invasion is less clear. Red light and speeding cameras are only placed in locations which are already in public, where one can already be seen. The greater permanence of the camera's recording may incline a person to restrain her eccentricities more than usual, but publicly placed cameras may be the kind of privacy invasion to which humans can adapt.

[95] The degree of harm surveillance causes thus depends on what technology is being used and where the surveillance is occurring.[194] Society and individuals' interests in avoiding these harms are relevant even when an invasive technology is being used successfully to enforce laws that all agree with, for, as Nagel argues, society cannot function without sufficient space to be one's private self.

C. BALANCE OF GOVERNMENT AND INDIVIDUAL POWER

[96] A final concern is that using technology to enforce laws will unwisely shift power to the government and from the individual. This notion of a "balance of power" between the government and its citizens is evoked in the Second Amendment.[195] Its meaning, concerning the "right of the people to keep and bear arms,"[196] has undergone much consideration. While most federal appellate courts have stated that the amendment is a "collective right" that only protects the private possession of weapons in connection to the function of a state citizen's militia,[197] the

[194] Other privacy concerns, such as the release of embarrassing secrets to the public (say, a traffic light camera photo of a politician and his mistress) or tracking individuals with unpopular beliefs are somewhat beyond the scope of this section, however a discussion of several possible abuses of the technologies mentioned herein can be found *supra* Part IV Section C.

[195] ZITTRAIN, *supra* note 9, at 116.

[196] U.S. CONST. amend. II.

[197] *See, e.g.*, Silveira v. Lockyer, 312 F.3d 1052, 1092 (9th Cir. 2002); Gillespie v. City of Indianapolis, 185 F.3d 693, 710 (7th Cir. 1999); United States v. Wright, 117 F.3d 1265, 1273–74 (11th Cir.1997); United States v. Rybar, 103 F.3d 273, 286 (3d Cir. 1996); Love v. Pepersack, 47 F.3d 120, 124 (4th Cir. 1995); United States v. Hale, 978 F.2d 1016, 1019-20 (8th Cir. 1992); United States v. Oakes, 564 F.2d 384, 387 (10th Cir. 1977);

D.C. Circuit has recently joined the Fifth Circuit and a number of state courts in holding that the Second Amendment protects an individual's right to keep and bear arms.[198] One rationale for allowing individuals to keep firearms is to maintain the people's ability to resist tyrannical government.[199] In order to prevent abuse of government power, one might believe not only in separation and balance of powers among the legislative, executive, and judicial branches, but also in the need for a balance of power between the government and the people themselves. This sentiment is present not only in some interpretations of the Second Amendment, but also in the limited powers of Congress[200] and in the Tenth Amendment.[201]

[97] Just as forbidding individuals from possessing firearms shifts power in favor of the government, using technology to enforce laws also shifts the balance of power between the government and the individual. Historically, the government has been made up of individuals, all of whom had to be willing to participate in law enforcement actions. To issue a speeding ticket, a police officer needed to pull over the speeding car, write the ticket, and appear in court if the ticket was challenged. This effort was roughly commensurate with the inconvenience to the driver of having to wait to receive the ticket and appear in court to challenge it.

[98] When a camera automatically issues tickets without an element of human discretion, however, the balance of power is shifted. The government trivially exerts its power—no one even has to look at the tickets as they are being mailed out. The alleged perpetrator receives a ticket in the mail, stating that some amount must be paid or the perpetrator

---

United States v. Warin, 530 F.2d 103, 106 (6th Cir. 1976); Cases v. United States, 131 F.2d 916, 921-23 (1st Cir. 1942).

[198] Parker v. District of Columbia, 478 F.3d 370, 395 (D.C. Cir. 2007); *see also, e.g.*, United States v. Emerson, 270 F.3d 203, 264–65 (5th Cir. 2001); Hilberg v. F.W. Woolworth Co., 761 P.2d 236, 240 (Colo. Ct. App. 1988); Brewer v. Commonwealth, 206 S.W.3d 343, 347 n. 5 (Ky. 2006); State v. Blanchard, 776 So.2d 1165, 1168 (La. 2001); State v. Nickerson, 247 P.2d 188, 192 (Mont. 1952); State v. Williams, 148 P.3d 993, 998 (Wash. 2006); Rohrbaugh v. State, 607 S.E.2d 404, 412 (W. Va. 2004).

[199] *Parker*, 478 F.3d at 395.

[200] *See* U.S. CONST. art. I, § 8.

[201] "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." U.S. CONST. amend. X.

must show up in court. In court, the evidence is the photographs or the video; a police officer need not take the time out of his day to testify as to what he saw. Similarly, the RIAA could choose to send notice and takedown letters automatically with minimal human oversight if their web crawlers became more accurate.[202] The provider of the allegedly infringing content would have to explain that the use of copyrighted material was fair, that there was some mistake, or that the material was accessed under one of the DMCA's exceptions.[203]

[99] The procedural safeguards of the court system may provide some insulation from this imbalance. The Minnesota Supreme Court, for instance, recently struck down a red light camera program as being in conflict with Minnesota state law, which preempts Minnesota traffic laws.[204] Under the ordinance describing the camera program, the owner of a car caught speeding was presumptively guilty of a misdemeanor.[205] However, Minnesota law provided that a defendant be "presumed innocent until proven guilty beyond a reasonable doubt . . . ."[206] The problem, the court explained, was that the presumption that the owner was the driver eliminated the presumption of innocence and shifted the burden of proof from the government to the defendant.[207] As a result of the decision, even if the cameras continue to be used, the government's power to prosecute traffic violations will be diminished and closer to the power of individuals in defensive postures.

[100] While courts may correct certain shifts in the balance of power, other government initiatives may be more difficult to challenge. In *The Company v. United States*, a company that provides an OnStar-like

[202] According to the RIAA, an individual looks at every letter before it is sent. McCullagh, Threatening Letter, *supra* note 54.
[203] *See, e.g.*, 17 U.S.C. § 1201(d) ("Exemption for Nonprofit Libraries, Archives, and Educational Institutions."); 17 U.S.C. § 1201(e) ("Law Enforcement, Intelligence, and Other Government Activities."); 17 U.S.C. § 1201(f) ("Reverse engineering . . . to achieve interoperability of an independently created computer program with other programs . . . ."); 17 U.S.C. § 1201(g) ("Encryption research."); 17 U.S.C. § 1201(i) ("Protection of Personally Identifying Information.").
[204] State v. Kulhman, 729 N.W.2d 577, 582 (Minn. 2007).
[205] *Id.* at 579.
[206] MINN. R. CRIM. P. 23.05, subd. 3 (1990).
[207] *Kuhlman*, 729 N.W.2d at 583.

system[208] for cars anonymously brought suit, objecting to the FBI's use of the system to eavesdrop on suspected criminals.[209] The FBI had not merely eavesdropped on telephone conversations using the system, but rather had remotely reprogrammed the microphone so all conversations in the car could be overheard.[210] The company believed they were not legally required to comply with the district court order to allow eavesdropping.[211] If the company had not objected, there may not have been a way for the suspects in the car to object, in large part because they had no way of knowing the eavesdropping program existed.

[101] Before tethered appliances, the exercise of government power was checked by the many who actively participated in the programs, both as agents of the government and as cooperating private parties.[212] In *The Company*, only the company was in a position to challenge the government's behavior. As surveillance becomes more automated, fewer and fewer parties will be in this position. In effect, the popularity of tethered appliances "diminishes the ability of a rule to attain legitimacy as people choose to participate in its enforcement or at least not stand in its way."[213]

[102] James Wilson explained at the Constitutional Convention, "[l]aws may be unjust, may be unwise, may be dangerous, may be destructive; and yet not so unconstitutional as to justify the Judges in refusing to give them

---

208

> Each System console has three buttons: (1) an emergency button, which routes customers' calls to the Company; (2) an information button, which routes customers' calls to the other company that assists the
>
> > customer with navigation; and (3) the roadside assistance button, which routes customers' calls to the other company for assistance in getting on-site service for vehicles. The System automatically contacts the Company if an airbag deploys or the vehicle's supplemental restraint system activates.

Id. at 1134.

209 The Company v. United States, 349 F.3d 1132, 1133 (9th Cir. 2003).

210 *Id.* at 1137-38.

211 *Id.* at 1143.

212 *See* ZITTRAIN, *supra* note 9, at 117-18.

213 *Id*.

effect."[214] The ability of individuals to disobey or refuse to enforce laws can provide lawmakers with the pressure and incentive to re-evaluate the wisdom of laws. Federal alcohol prohibition was eliminated not only due to widespread disobedience, but also due to the apathy of many non-drinkers who did not report bootleggers and the willingness of some law enforcement officials to turn the other cheek.[215] Today, California state police officers' unwillingness to help enforce federal law prohibiting the use of "medical marijuana" is creating pressure to change federal drug laws.[216] This type of pressure is more difficult to create when laws are enforced automatically. Systems of "perfect prevention" will eliminate the opportunity for civil disobedience entirely, and systems of "perfect surveillance" will require far fewer officials and private individuals to go along with the program. Overall, perfect enforcement will decrease society's ability to gain the momentum needed to bring about changes to unjust or unwise laws.

VII. CONCLUSION

[103] This Article has cataloged and explored several concerns one might have about using technology to enforce law, embracing the use of technology in some cases and repudiating it in others. Each concern was illustrated with examples ranging from traffic cameras to web crawlers to identification cards. Yet, the use of such a catalog is not principally in its application to these particular cases, but in what might be learned and applied to those we encounter in the future.

[214] 2 THE RECORDS OF THE FEDERAL CONVENTION 73 (Max Ferrand ed., 2d ed. 1911).
[215] *See* Digital History, http://www.digitalhistory.uh.edu/database/article_display.cfm?HHID=441 (last visited Mar. 29, 2008).
[216] *See generally* A. Christopher Bryant, *The Third Death of Federalisim*, 17 CORNELL J.L. & PUB. POL'Y 101 (2007).

[104] With a view towards these future, unknown cases, this article concludes not with a summary, but with a list of questions that policymakers and technologists can use to determine whether the use of a technology to enforce law is wise.

1. Is it feasible to use the technology for the proposed purpose?
2. Will the technology generate an unreasonably high number of false-positives or false-negatives? If so, can these mistakes be corrected with the addition of a human element?
3. What are the potentials for abuse? What are the possible side-effects of the technology being used? Can these potentials be eliminated without making the technology ineffective?
4. Might the use of the technology trigger a First or Fourth Amendment violation?
5. If the technology's use is constitutional, might the use still unwisely curtail speech or fair uses?
6. If the technology is designed to perfectly prevent a law violation, are there any circumstances under which it would be important or necessary to violate the law for a greater good?
7. Is the elimination of discretion in the law's enforcement problematic?
8. Does the technology intrude on one's private space enough to chill eccentric behavior or affect one's ability to function publicly?
9. Does the use of the technology unwisely shift the balance of power between the government and its citizens?

[105] Questions 1 and 4 are deal-breaking; any program must be feasible and must be constitutional. The other questions are factors that may often cut in opposing directions, ultimately requiring a decision-maker to make choices based on the totality of the circumstances. If these questions are considered, such choices will be informed and justified, allowing technology to be used without abusing those it is employed to protect.