ARTICLE

PHOTO RADAR ENFORCEMENT: A BRIEF STALL ON A SLIPPERY SLOPE?

ANDREW ASKLAND*

INTRODUCTION

In 1964, a Dutch company introduced the first speed camera, the incidental product of a rally driver's efforts to accurately monitor his speed on a racetrack.[1] Shortly thereafter, the company introduced a red light camera.[2] Speed enforcement cameras evolved with the introduction of radar in the 1970s and expanded significantly with the adoption of digital cameras in the 1990s.[3] Driven by pressure to reduce large budget deficits (abetted by promises of windfall profits from third-party contractors offering to install and manage photo radar equipment) while simultaneously improving roadway safety, state and local governments embraced photo radar enforcement in increasing numbers shortly after the 2008 recession in order to increase revenues.[4] Although some officials acknowledged a revenue motive for the increased use

* Director, Center for Law, Science and Innovation, Arizona State University, Sandra Day O'Connor College of Law; Ph.D., Philosophy, University of Colorado-Boulder; J.D., University of Maryland-Baltimore.

[1] *Experts in Traffic Enforcement*, GATSO, http://www.gatso.com/upload/9529429274ed4e162ca5b3.pdf (last visited Oct. 22, 2012).

[2] *Id.*

[3] *Id.*

[4] *See* Patrick O'Donnell, *Garfield Heights Mayor Thomas Longo Looks at Traffic Cameras for Money to Erase Budget Deficit*, CLEV. PLAIN DEALER, March 28, 2009, http://blog.cleveland.com/metro/2009/03/garfield_heights_mayor_thomas.html; Nathan Gonzalez, *Speed, Red-light Cameras Save Lives But Lose Money*, ARIZ. REPUBLIC, March 5, 2010, http://www.azcentral.com/community/mesa/articles/20100305mesa-photo-radar.html; *Goldman Sachs Invests in American Traffic Solutions*, BUS. WIRE, Sept. 25, 2008, http://www.businesswire.com/news/home/20080925005840/en/Goldman-Sachs-Invests-American-Traffic-Solutions; Karen Pate, *More Sophisticated Photo Radar Coming to Beaverton*, THE OREGONIAN, June 17, 2008, http://blog.oregonlive.com/breakingnews/2008/06/more_sophisticated_photoradar.html; *Mayor Unveils New "Speed Van"*, SEATTLE CRIME NEWS (March 10, 2008), spdblotter.seattle.gov/2008/10/20/mayor-unveils-new-speed-van/; Paul Davenport, *Ariz.'s Napolitano Defends Highway Photo Radar Proposal*, INS. J., Feb. 15, 2008, http://www.insurancejournal.com/news/west/2008/02/15/87408.htm; *REDFLEX Speed Enforcement*, REDFLEX TRAFFIC SOLUTION, http://www.redflex.com/index.php/en/solutions/redflex-speed-enforcement (last visited Jan. 21, 2013).

of photo radar,[5] most government officials stressed the promotion of public safety to justify photo radar, a response inspired in part by sharp expressions of public concern about revenue inspired enforcement, and also by uneven revenues generated from enhanced photo radar enforcement.[6] There are ample good reasons to use photo radar to enforce speed limits, but the widespread use of the technology raises a variety of privacy concerns. Using the experiences of Arizona as an example, this Article argues that the privacy concerns raised by the widespread use of photo radar enforcement, as opposed to a more targeted use, outweigh the considerations supporting widespread use of the technology. The blind pursuit of increased revenue and mechanical enforcement of the law should not obscure the substantial burdens imposed upon privacy by an extensive system of photo radar enforcement.

Arizona adopted a state-wide photo radar enforcement program in October 2008, despite trepidation among some lawmakers about the public response,[7] but terminated the program less than two years later, in July 2010.[8] When Governor Janet Napolitano adopted the program, she acknowledged that a significant purpose was to generate revenue to close an unprecedented budget revenue shortfall.[9] She also cited road safety, and the state did see a nineteen percent drop in fatal collisions in the first nine months of the program.[10] The program was authorized by changes in the governing Arizona statute, which also provided that speeding citations issued pursuant to the newly instituted program would not be considered a violation for the purposes of license revocation or suspension—meaning that no points were assessed for violations.[11] Governor Jan Brewer ended the state-level program by allowing the contract with the third-party contractor to expire, but photo radar

[5] *See* O'Donnell, *supra* note 4; Davenport, *supra* note 4.

[6] *See* Gonzalez, *supra* note 4; Howard Fischer, *Napolitano Defends State Photo Radar Plan*, ARIZ. DAILY STAR, Feb.14, 2008 (noting that Gov. Napolitano defended the state's photo radar program, "saying it's just a happy coincidence that it will help her with the state budget deficit"). For a discussion of how acceptance of photo radar is affected by public perception of devices located to promote safety rather than enhance revenue, *see* AUDITOR-GENERAL, SPECIAL REPORT NO. 85: SPEED-DETECTION DEVICES, 2, 7, 11 (Nov. 2009), *available at* http://www.audit.tas.gov.au/publications/reports/specialreport/pdfs/specialrep85.pdf.

[7] Davenport, *supra* note 4.

[8] Randal C. Archibold, *First State to Adopt Photo Enforcement of Speed Law, Arizona Halts the Program*, N.Y. TIMES, July 16, 2010, at A12.

[9] Paul Davenport, *Budget Plan Includes Photo Enforcement of Speed Limits*, TUCSON CITIZEN, June 26, 2008

[10] *Id.*; Fischer, *supra* note 6.

[11] ARIZ. REV. STAT. ANN. § 41-1722 (2009) (West), *repealed by* 2011 Ariz. Legis. Serv. ch. 308.

enforcement programs in fourteen cities in Arizona remain unaffected.[12]

Photo radar relies upon first class mail to deliver citations, causing a few courts to balk at this form of process.[13] However, aside from service of process complications, no court in the state has ruled that photo radar enforcement of speeding laws is unconstitutional, or otherwise unlawful.[14] The downturn in the use of state-wide comprehensive programs of photo radar enforcement for speeding violations in Arizona, as in other locations, can be attributed to several concerns about its expanded use, including the delegation of police powers to third-parties, enforcement fairness, service of process complications, negative public response, and revenue disappointments. Most photo radar enforcement is conducted by municipal rather than state authorities and their policies regarding the use of the technology vary widely and are affected by many variables, although the issues that arose in Arizona feature prominently among them.[15]

This Article first surveys several recurring criticisms of widespread photo radar enforcement and identifies likely changes in practice that might defuse those criticisms.[16] It then discusses the problem of over-inclusiveness in enforcing laws intended to target major rather than minor violations.[17] This Article then examines the private-public dichotomy that dominates legal analysis of how the law responds when private matters are exposed to public view.[18] It describes three factors that tilt this response toward diminished privacy protections: apprehensions about privacy protection as an impediment to the War on Terror; the shaping (mostly by lobbyists) of legislation ostensibly intended to address privacy concerns to minimally affect market prerogatives; and the reluctance of judges, given an uneven mosaic of legal sources for the protection of privacy, to recognize or prioritize privacy rights and interests.[19] This Article closes with some speculations about future use of

[12] Casey Newton, *Arizona to Eliminate Speed-Enforcement Radar on Freeways*, ARIZ. REPUBLIC, May 6, 2010, http://www.azcentral.com/news/articles/2010/05/06/20100506arizona-to-eliminate-speed-cameras.html.

[13] *See, e.g.*, Tonner v. Paradise Valley Magistrate's Court, 831 P.2d. 448, 449 (Ariz. Ct. App. 1992).

[14] Paul McNaughton, *Photo Enforcement Programs: Are They Permissible Under the United States Constitution?*, 43 J. MARSHALL L. REV. 463, 470, 489 (2010); *see* Thomas M. Stanek, *Photo Radar in Arizona: Is It Constitutional?*, 30 ARIZ. ST. L.J. 1209, 1229–41 (1998).

[15] NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., DEP'T OF TRANSP., SPEED ENFORCEMENT CAMERA SYSTEMS: OPERATIONAL GUIDELINES (2008), *available at* http://www.nhtsa.gov/DOT/NHTSA/Traffic%20Injury%20Control/Articles/Associated%20Files/810916.pdf.

[16] *See infra* Parts I & II.

[17] *See infra* Part III.

[18] *See infra* Part IV.

[19] *See infra* Part V.

photo radar enforcement and other motor vehicle-focused surveillance technologies.[20]

I. PROBLEMS WITH WIDESPREAD PHOTO RADAR ENFORCEMENT.

Despite the potential for increased roadway safety and revenue, photo radar enforcement programs, such as the program adopted in Arizona, suffer from significant drawbacks. First, the delegation of law enforcement to third-party contractors is objectionable on several grounds. The training and supervision of individuals who operate the programs are outsourced to third-party contractors who are not directly answerable to elected officials in the same way as police personnel. The attenuation of the chain of responsibility is problematic because it shelters actors performing police power functions behind contractual provisions that are drafted to promote and protect the third party's priorities. Flexibility to respond to citizen feedback about the program is often stymied by the terms of the contract negotiated with these third parties. Moreover, the motivation of these third parties is primarily profit maximization, and that motivation can shapes their policies because their earnings are often directly tied to the volume of citations that their devices generate. Small calibration changes in setting the devices can significantly increase the enforcement yield, and it would be difficult to eliminate the bias (conscious or unconscious) in favor of identifying violations when benefits are so obviously tied to volume.[21] One court, addressing photo enforcement of red light violations, stated that the "potential conflict created by a contingent method of compensation . . . undermines the trustworthiness of the evidence."[22]

Second, the challenge of linking driver photographs to data for the vehicle's registered owner prompted widespread unfairness complaints about enforcement because, for example, vehicles registered to corporations were not ticketed; female drivers of vehicles registered to males were not ticketed (and vice versa); out-of-state vehicles were not ticketed; rental vehicles were not ticketed; vehicles towing trailers or boats were not ticketed; drivers whose heads were turned or tilted or otherwise obstructed (whether by accident or on purpose, as in some cases drivers wore masks) when the enforcement photograph was taken were not ticketed; and vehicles with dirty license plates or plate covers were not ticketed.[23] Inconvenience and expense largely explain

[20] *See infra* Part VI.

[21] *See Arizona Officials Mislead Public on Photo Radar Ticket Review*, THENEWSPAPER.COM (Sept. 2, 2009), http://www.thenewspaper.com/news/28/2895.asp.

[22] State v. Allen, No. 57927SD (Cal. Super. Ct. 2001), *available at* http://alexandrialawlibrary.com/red57927.dismiss-ord-080901.htm.

[23] Stanek, *supra* note 14, at 1226. *See also* DEBBIE DAVENPORT, ST. OF ARIZ. OFF. OF THE AUDITOR GEN., DEP'T OF PUB. SAFETY PHOTO ENFORCEMENT PROGRAM (Jan. 19, 2010) (estimating that forty-seven percent of its photographs were rejected), *available at*

these failures to pursue enforcement, but from the perspective of fairness and equity, these justifications may appear objectionably arbitrary.[24] If speeding was really the focus of concern, then the state should have made a concerted effort to improve the effectiveness of enforcement by attempting to overcome the obstacles preventing identification.

A related fairness concern focuses on driver response to permanently stationed radar enforcement devices. Drivers who regularly travel routes where there are permanent devices learn to slow down as they approach the device, whatever speed they were driving before the approach.[25] In addition to the increased dangers arising from these sudden slow downs, there is also the fairness complaint that drivers who are unaware of the fixed devices, but are otherwise driving at the prevailing speed, are ticketed while drivers driving faster than the prevailing speed who brake for the devices, perhaps dangerously, are not ticketed. Enforcement may seem a matter of gamesmanship rather than the function of a rationally tailored methodology.

While these fairness complaints provide fodder for public dissatisfaction with photo radar enforcement programs, they are likely insufficient to support an equal protection or a due process challenge to particular programs.[26] Further, the privacy interest at stake has not been identified as a fundamental right, which would qualify it for subjective due process protection.[27] Because of this, the state's compelling interest in roadway safety will likely overcome any fairness complaints about shortcomings in the implementation of these programs.[28]

An additional potential problem with photo radar is based on the issue of service of process. Service of process to photographed drivers can prove problematic and expensive, as courts sometimes will not accept first class mail delivery of citations as adequate service.[29] Some courts refused to accept mail delivery of citations as a substitute for a police officer issuing a citation at the scene of the infraction, or to presume that the registered owner of the vehicle was operating the vehicle when a violation was detected.[30] Prosecutors were

http://www.azauditor.gov/Reports/State_Agencies/Agencies/Public_Safety_Department_of/Performance/10-02/10-02.pdf.

[24] Stanek, *supra* note 14.

[25] *See* VA. TRANSP. RES. COUNCIL, RESEARCH REPORT: THE IMPACT OF RED LIGHT CAMERAS (PHOTO-RED ENFORCEMENT) ON CRASHES IN VIRGINIA (2007), *available at* http://www.virginiadot.org/vtrc/main/online_reports/pdf/07-r2.pdf.

[26] Lisa S. Morris, *Photo Radar: Friend or Foe?*, 61 UMKC L. REV. 805, 810–815 (1993).

[27] *Id*. at 813.

[28] *See* Mackey v. Montrym, 443 U.S. 1, 17 (1979).

[29] *See, e.g.*, Tonner v. Paradise Valley Magistrate's Court, 831 P.2d. 448, 449 (Ariz. Ct. App. 1992).

[30] *See* People v. Hildebrandt, 126 N.E.2d. 377, 379 (N.Y. 1955). This was the first case

forced to secure service processors or request court authorization to post citations on door fronts to satisfy the service problems. These alternative means of making service imposed delays and increased costs and further diminished public and official enthusiasm for the programs.[31]

However, this complication may prove less problematic if and when large-scale photo radar enforcement programs are reintroduced. As elaborated below, there is precedent for requiring a registered motor vehicle owner either to report the identity of the vehicle operator when a violation occurs or to bear the burden of that violation. That obligation can be spelled out more clearly if and when a state reauthorizes a widespread photo radar enforcement program. Indeed, the judges who were reluctant to accept mailed process may have been affected by the general unpopularity of the photo radar enforcement programs, but were unready to rely upon legal or policy arguments that had not yet solidified as judicially recognizable or dispositive.[32]

Public response to photo radar, particularly its widespread use, is generally negative, and many conservatives who usually support law-and-order initiatives have joined in the criticisms of the intrusive nature of the program.[33] Some polls suggest support for the programs, particularly polls funded by the sponsors of the programs.[34] As is often the case with public opinion surveys, the framing of the question often predicts the tenor of the response.[35] Aside

where a court refused to accept the presumption that the owner of a vehicle is the operator of that vehicle when a device detects a violation. *See id*. at 399.

[31] Jim Walsh, *Mesa's Photo Radar System Not a Money Maker*, ARIZ. REPUBLIC, Mar. 11, 2009, http://www.azcentral.com/community/mesa/articles/2009/03/11/20090311mr-photoradar0311.html.

[32] One expression of judicial qualms about photo enforcement can be seen in a decision of a California appellate court requiring thirty days notice at each intersection with a red light camera before the camera was activated. People v. Park, 115 Cal. Rptr. 3d 337 (Cal. App. Dep't Super. Ct. 2010) *disapproved of by* People v. Gray, 139 Cal. Rptr. 3d 489 (Cal. Ct. App. 2012).

[33] The "primary purpose" of the Insurance Institute for Public Safety has been to encourage government agencies to issue more tickets in the name of safety. "Government agencies are similarly motivated to install cameras at budget time and become lukewarm to the idea if the profits fail to materialize. The public is never lukewarm on the issue; its response has been uniformly negative." Editorial, *Red-light-Camera Flop*, WASH. TIMES, June 30, 2011, http://www.washingtontimes.com/news/2011/jun/30/red-light-camera-flop/.

[34] *See* Caroline J. Rodier et al., *Automated Speed Enforcement in the U.S.: A Review of the Literature on Benefits and Barriers to Implementation* 10–14 (Inst. of Transp. Studies, Univ. of Cal. at Davis 2007), *available at* http://www.its.ucdavis.edu/?page_id=10063&pub_id=1097 (summarizing various studies suggesting public support for photo radar enforcement); R.A Retting, *Speed Cameras—Public Perceptions in the U.S.*, 44(3) TRAFFIC ENGINEERING & CONTROL 100, 100–01 (2003) (noting public support for the photo radar program in Washington, D.C.).

[35] *See* Christine Jolls et. al., *A Behavioral Approach to Law and Economics*, 50 STAN. L.

from public surveys, the public has often voted against the programs.[36] By 2010, fifteen states and eleven cities had banned or restricted the use of photo radar enforcement.[37]

Complaints about the programs arise not only from violators, but also from the general populace and politicians who decry the invasive nature of administering speed limits with photo radar. It has been a contentious issue in various local elections.[38] The photographs present a special concern because they make drivers unwilling subjects of public scrutiny. For this particular privacy-invasive technology, the momentum of the progressively enveloping surveillance society has met resistance, at least for the present.

Perhaps most tellingly, the revenue projections for widespread photo radar enforcement were unrealized and future revenues were projected to decrease.[39] State budgets were in peril in the aftermath of the mortgage banking industry debacle, but the crisis mode passed. Anticipated revenue enhancements were more carefully reviewed as the crisis was averted and relevant data became available.[40] Given that the abrupt increase in use of photo radar was rationalized in part by substantial projected revenue increases, when the projections proved unduly optimistic, an important rationale for the surge in photo radar use failed.[41]

A separate concern about all photo radar enforcement is that it does not stop any violations that it records. The devices photograph an event, but cannot intervene to apprehend the violator. If the photographed violation is compounded by other violations, for example, driving under the influence of alcohol or aggressive driving, a photograph will not capture facts relevant to those other violations (which an on-the-scene arresting officer would observe and could charge).

For these multiple reasons, widespread photo radar programs operated by third-party contractors have generally waned across the country. However, the use of photo radar remains a popular enforcement tool and safety concerns are most often cited to justify its use, though the programs that persist usually also produce at least small revenue gains. While photo radar is still useful to

---

REV. 1471, 1536 (1998); *see generally* BEHAVIORAL LAW AND ECONOMICS (Cass Sunstein ed., 2000).

[36] Wayne Baker, *'Photocop' Didn't Play in Peoria*, CHI. TRI., March 21, 1991, http://articles.chicagotribune.com/1991-03-21/news/9101250641_1_photocop-traffic-monitoring-technologies-photo-radar.

[37] Raymond Hernandez, *Traffic-Camera Debate Heats Up Campaign Trails*, N.Y. TIMES, Aug. 7, 2010, at A14, http://www.nytimes.com/2010/08/08/us/08traffic.html.

[38] *Id*.

[39] Gonzalez, *supra* note 4

[40] JJ Hensley & Alia Rau, *Pressure Mounts to End Speed Camera Program in Arizona*, ARIZ. REPUBLIC, Jan. 23, 2010.

[41] *Id*.

enforce speed limits, enforcement has largely reverted to police control and photo radar programs no longer aim, at least as a controlling priority, to identify a maximal number of violators in order to significantly supplement income for local and state coffers.[42]

II. DEFUSING PROBLEMS WITH WIDESPREAD PHOTO RADAR ENFORCEMENT.

The dampening of the enthusiasm for widespread photo radar enforcement programs may not be permanent. It may be reintroduced at a later time, perhaps when some of the administrative kinks in its surge-related formatting are solved and the expanding surveillance practices in other aspects of the national culture numb privacy concerns about photo radar technologies. Some of the problems with its earlier implementation can likely be remedied to temper at least some criticisms. The use of regular police personnel, rather than third-party contractors, to staff and manage photo radar program would address a major complaint. Emphasizing increased safety, rather than increased revenue, to justify photo radar (and basing the placement of photo radar on safety considerations rather than considerations of revenue) would likely make it more palatable. Photo enforcement might be touted as a means to remove the potential bias of the individual police officers issuing citations. Various radar enforcement programs aiming at widespread enforcement forestalled criticisms by carefully drafting third party contracts and emphasizing police oversight; though the programs might employ civilian operators, they are not directed by third-party contractors whose earnings are directly related to the number of citations issued.[43]

Changes to motor vehicle registration regulations to facilitate matching speeding drivers with registered vehicles would reduce complaints about implementation fairness. Corporations that register vehicles for their direct use (or rent vehicles to others) might be required to maintain use records to help identify speed violators. Registered owners might be held responsible for illegal use of their vehicles unless they identify the driver of their vehicle when it is used to violate traffic laws.[44]

---

[42] Ryan Randazzo, *Traffic Cameras Not Profitable for Cities Across Arizona*, ARIZ. REPUBLIC, July 3, 2011, http://www.azcentral.com/business/articles/20110703traffic-camera-arizona-city-profit.html.

[43] For example, the Rockville City Police in Montgomery County, Maryland, highlights its hiring of new police officers "solely dedicated to traffic enforcement" in its assessment evaluation of its photo radar speed enforcement. ROCKVILLE CITY POLICE, SAFE SPEED PROGRAM EVALUATION (July 23, 2009), *available at* http://www.rockvillemd.gov/police/rcpd_safe_speed_program_eval_7-23-09.pdf.

[44] *See, e.g.*, British Columbia Motor Vehicle Act, R.S.B.C. 1996, c. 318, § 83.1(2) (Can.) (current through Jan. 16, 2013) ("The owner of a motor vehicle is liable for [a violation] if evidence of the contravention was gathered through the use of a prescribed speed monitoring device. . . [or]. . . prescribed traffic light safety device . . . . An owner is not

Such impositions on registered motor vehicle owners would constitute an arguably minor elaboration of the regulatory state. Ownership of a vehicle might be conditioned on responsiveness to written notice that the vehicle has been used to violate traffic laws and appearance at a hearing might be required to contest proposed registration suspension or revocation.[45] Driving is regarded as a privilege rather than a right, and a privilege can be conditioned by the state so long as the conditions are reasonable.[46] In an era that is haunted by terrorism threats and succumbs to progressively more invasive surveillance technologies, the plasticity of such a reasonableness standard may readily accommodate these "driver liability" (sometimes called "tattle or pay") impositions upon vehicle registration. Appellate courts might well view a legislatively imposed burden to report on illegal vehicle use to be reasonable.

Drivers are already required to maintain a current mailing address with the motor vehicle administration to receive notices relating to their licenses, for example, renewals, proposed suspensions, etc., and vehicle owners are similarly required to maintain that information for vehicle registration renewals.[47] First-class mail is generally deemed adequate notice for these purposes.[48] The use of first class mail is already the current practice in Canada and in some states for traffic violations.[49] When pressed, courts may be reluctant to issue bench warrants in situations where violators fail to appear in court when summoned by mail.[50] A solution to this reluctance is that courts may issue summons to be served by sheriff upon violators who fail to respond to a mailed summons. There may be a presumption that mailed summons have been delivered which would enable states to impose the costs of service of the summons by a sheriff upon the violator unless it is affirmatively demonstrated

liable [for a violation] if the owner establishes that (a) the person who was, at the time of the contravention, in possession of the motor vehicle was not entrusted by the owner with possession, or (b) the owner exercised reasonable care and diligence in entrusting the motor vehicle to the person who was, at the time of the contravention, in possession of the motor vehicle."); *see also* O'Halloran v. United Kingdom, App. Nos. 15809/02 & 25624/02, Eur. Ct. H.R. (2007) (upholding the United Kingdom's requirement that a vehicle owner identify the driver of that vehicle at the time a traffic violation occurred).

[45] Morris, *supra* note 26, at 819; *see* Randa Heifez, *Are Red Light Cameras in Georgia Overexposing the Public and Undermining Privacy Rights?*, 2 J. MARSHALL L. REV. 245 (2009).

[46] *See* Hendrick v. Maryland, 235 U.S. 610, 624 (1915).

[47] State v. Cifelli, 155 P.3d 363 (Ariz. Ct. App. 2007).

[48] *Id*. at 367–68.

[49] *See, e.g.*, British Columbia Offense Act, R.S.B.C. 1996, c. 338, § 14(6) (Can.) (current through Jan. 16, 2013) (allowing tickets for violations identified with photo radar devices to be delivered via mail); TENN. CODE ANN. § 55-8-198 (2012) (prescribing that violations detected by photo radar devices be sent by mail).

[50] *See* Tonner v. Paradise Valley Magistrate's Court, 831 P.2d. 448, 448 (Ariz. Ct. App. 1992).

that the mail was not delivered.

III. A SPECIAL PROBLEM OF OVER-INCLUSIVENESS.

The prospect of expanding the enforcement of motor vehicle laws to Orwellian extremes is promoted by continuing reductions in the cost of the technology and the progressive diminution of public expectations about privacy, especially in light of changing views about what monitoring of behavior is reasonable. Law enforcement has costs and general deterrence can reduce those costs. Focusing on the clearest violations of the law sends a signal to those whose violations are minor and unprosecuted that they should not broaden their violations, lest they cross the enforcement threshold and attract prosecution.[51] It may be prohibitively expensive to identify and prosecute all violations, but pursuing clear and major violations deters minor violators against major violations and accordingly reduces social costs.[52]

If enforcement costs are significantly reduced, law enforcement may be tempted to pursue lesser violations. On the one hand, more enforcement can be better when it is clear that the lesser violations impose social costs. On the other hand, more enforcement can press on the evaluation of the social costs of the lesser violations. It is easier to agree that a category of behavior is wrong if we limit enforcement to egregious examples. Agreement may be less easily reached if many socially acceptable instances of that behavior are reassessed to fit within the definition of a wrong that will be prosecuted. This is especially true when the wrong at issue is not a *malum in se*, but rather a *malum prohibitum*, meaning wrongful not on account of an intrinsic quality (a natural evil), but only because of statutory or regulatory stipulations.[53]

We may not want to enforce every law in each instance in which the letter of the law indicates a violation. We intend discretion to be part of the enforcement of laws that cannot be exactly worded to distinguish between the acts that are the focus of legislative concern and the acts that may technically violate the law, but were not intended to be covered.[54] For example, how drunk and disorderly must one be to qualify as an offender? Clearly someone might qualify as inebriated without posing a threat as generally encompassed by drunk and disorderly laws. One might also be disorderly, but only briefly and in a setting which does not pose a threat or inconvenience to others and thus evade arrest and prosecution despite being technically in violation. On the other hand, in a volatile situation an officer might reduce the threshold for disorderly to pre-empt a potentially dangerous cascade of events. If we reduced drunk and disorderly to a breathalyzer assessment of sobriety and

---

[51] H.L.A. HART ET AL., THE CONCEPT OF LAW 120 (3d ed. 2012).

[52] H.L.A. HART, PUNISHMENT AND RESPONSIBILITY 128 (2d ed. 2008).

[53] RONALD DWORKIN, LAW'S EMPIRE (1986).

[54] KENT GREENAWALT, LAW AND OBJECTIVITY 11 (1992).

decibel meter reading of any vocal outburst above a specified volume, we would apprehend more individuals than the statute or the legislature that enacted it intended.[55] We may also negatively affect the public perception of drunk and disorderly statutes as appropriate remedies for problems that are inexactly circumscribed within the statute's language. We probably do not intend that anyone who is inebriated and deviates briefly from normal behavior (however we decide the boundaries of normal behavior) in a public place is a lawbreaker. Continual monitoring of public streets might provide evidence of technical violations that would undermine confidence in the governing statute and in law enforcement generally.[56]

IV. THE PRIVATE-PUBLIC DICHOTOMY IN PRIVACY LAW.

Rather than debate these several strains of criticisms of photo radar enforcement, this paper instead focuses on the privacy-invasive aspects of the technology when it is adopted for widespread use. It argues, perhaps quixotically, that widespread use of photo radar is objectionable because it stretches the justification for narrowly tailored photo radar use beyond its boundaries without acknowledging the changed dimension of the burden that this expanded use imposes upon personal privacy. The larger burden that widespread photo radar imposes should be assessed on the basis of the benefits and costs of that expanded use. Arguably, those burdens are substantial and would not be justified by either the two prong test of *Katz*, the currently governing matrix that looks for an actual (subjective) expectation that society recognizes as "reasonable,"[57] or other tests that might be offered as alternatives to *Katz* when these tests concede appropriate weight to privacy as either a right or a compelling interest.

Widespread use of photo radar transforms operating a motor vehicle into an unduly regulated activity because it is a fully visually monitored activity. Operating a motor vehicle ceases to be the movement of a presumably privacy-protective person, and is instead the maximally monitored activities of a member of a suspect class, similar to a convicted criminal, perhaps as a probationer, who has forfeited civil rights on account of prior grievously wrongful conduct (Beware Jeremy Bentham's Panopticon!).[58] Whatever the merits or demerits of photo radar enforcement solely focused on historically problematic stretches of roadway, the unchecked expansion of its use portends qualitatively different challenges that significantly and objectionably burden

[55] JOSEPH RAZ, THE AUTHORITY OF LAW 120 (2d ed. 2009).

[56] HART ET AL., *supra* note 51.

[57] Katz v. United States, 389 U.S. 347, 353 (1967).

[58] MICHEL FOUCAULT, DISCIPLINE AND PUNISH 201–02 (Alan Sheridan trans., Vintage Books ed. 1979) (1977) (discussing JEREMY BENTHAM, PANOPTICON (1787)) (noting the relevance of a prison designed to permit continual surveillance of prisoners who would not know whether they were being observed to contemporary social practices).

personal privacy. A narrowly focused use of photo radar is distinguishable from its widespread use and the descent down a slippery slope from one to the other is avoidable if each proposed use is weighed against its effects upon privacy. A linear account of the evolution of photo radar use lends itself to slippery slope analogies. A stepped approach (with multiple gradations of the tradeoffs between competing values) can better accommodate thresholds and boundaries.

The all-or-nothing approach that is promoted with a mechanical enforcement of law tracks a general inadequacy in phrasing protections for privacy. While clarity, predictability, and ease of administration argue for sharp distinctions, complex problems are often ill-suited to simple solutions. Despite periodic dissent, such as Justice Marshall's admonition in the context of police use of pen register devices without a court order that "[p]rivacy is not a discrete commodity possessed absolutely or not at all,"[59] and Justice Stevens' acknowledgement, in the context of a request to the Federal Bureau of Investigation for an individual's rap sheet listing information already largely a matter of public record that "the fact that an event is not wholly private does not mean that an individual has no interest in limiting disclosure or dissemination of the information,"[60] there is a longstanding tendency in court opinions and academic commentaries to view the movement from private to public as a movement across a threshold, beyond which complaints do not register or register only faintly. The occasional recognition of degrees of privacy is largely overwhelmed by simpler evaluations of the private-public boundary. One court famously opined that "[t]here can be no privacy in that which is already public,"[61] and the threshold determination that something is public is usually regarded as non-problematic. Once a private matter becomes public, crossing a fairly sharp dividing line, use of previously private matter is largely unconstrained. The sharpness of the boundary makes the distinction easier to enforce, thereby promoting judicial and enforcement economy, but it does not necessarily comport with widely shared expectations about when behavior qualifies as public. Furthermore, advances in information technologies and social media are rapidly exposing these disappointed expectations, for example, as users of social media discover that their messages can be accessed by a larger audience than they foresaw or can control.

The private-public distinction derives from Aristotle and his model of the virtuous man as a citizen of a *polis* engaged in public debates with fellow citizens. A man who did not engage in public debate was not wholly a citizen because he deprived himself of essential social bonds, but it was also the case

[59] Smith v. Maryland, 442 U.S. 735, 749 (1979).

[60] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 769 (1989) (quoting William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair Effective Law Enforcement?*, 23 U. KAN. L. REV. 1, 8 (1974–75)).

[61] Melvin v. Reid, 297 P. 91, 94 (Cal. 1931).

that the citizen required the repose of a private household to succor his mental strength and restore his spiritual equilibrium.[62] The separation of private and public spheres developed over time from a balance of solitude and intimacy embedded within social engagement into a dichotomy that precluded public interference in private affairs, but also justified public interference whenever the public threshold was crossed.[63]

This dichotomy disserves important values in cases where a social practice has both public and private aspects that are integral to that practice. For example, feminists criticize the dichotomy[64] because it can shelter abuses within the family from public scrutiny, such as the physical abuse of wives by their husbands that was ignored by courts that declined to interfere in private family matters.[65] Because courts perceived privacy in an either/or framework, meaning that either action in a family setting must be protected as private or exposed to public scrutiny, they opted to overlook misdeeds in the name of the sanctity of family privacy.[66] A less dichotomous view of such actions protects the integrity of the family and recognizes abuses that merit intervention.

Despite the potential for misuse, the public-private distinction is useful when it is better explicated and more artfully applied. The contrast between private and public is vital because it picks out two essential qualities of the human condition, the solitary consciousness of each individual and the ineluctable dependence of every human upon assistance from others, whether as a helpless infant, or an otherwise language-less brain (or mind, as you prefer), or a person reliant upon community and culture to define herself.[67] Even solitude relies upon thoughts articulated in a language shared with others and generally involves a review of one's place in a socially constructed world. Humans are intrinsically private *and* public; it is folly to expect a sharp boundary marking where a person crosses from one aspect of their nature to the other.

Privacy originates in the individual's consciousness and yet its shape depends upon practices that enable or retard its reach. Its core is consciousness that escapes direct observation, but its expression depends upon social practice. Privacy can be squeezed by a draconian, omnipresent surveillance or wallow self-absorbed in hyper-insulated isolation. Privacy should not be reduced to unexpressed thoughts, but instead should include stages of expression that

---

[62] ARISTOTLE, NICOMACHEAN ETHICS, Bk. VIII.

[63] Reva B. Siegal, *"The Rule of Love": Wife Beating as Prerogative and Privacy*, 105 YALE L.J. 2117 (1996).

[64] CATHERINE A. MACKINNON, TOWARDS A FEMINIST THEORY OF THE STATE (2d ed. 1991).

[65] State v. Rhodes, 61 N.C. 453, 459 (1868).

[66] Siegal, *supra* note 63, at 2167.

[67] Oscar H. Gandy, Jr., *Exploring Identity and Identification in Cyberspace*, 14 NOTRE DAME J.L ETHICS & PUB. POL'Y. 1085, 1097 (2000).

stretch from diary entries and confidential conversations to disclosures within a support group and Internet-mediated purchases of consumer goods.[68]

Our current privacy practices largely rely upon a dichotomous view of the private and the public. Once information about a person is publicly available, there are few limits to the permissible uses of that information. The so-called "third-party doctrine" is a noteworthy expression of this dichotomy-driven diminution of privacy protection. The doctrine arises from Supreme Court rulings in several contexts—including police access without a court order to records maintained by phone companies[69] and banks[70]—that Fourth Amendment protections against search and seizure do not encompass records that a person voluntarily turns over to a third party.[71] The effects of the third-party doctrine are harsh, given that our contemporary lifestyles rely upon services provided by third parties, such as banks, merchants, credit card companies, public service utilities, etc.[72]

The third-party doctrine reflects prevailing views about personal information held by third parties. If a person provides information to a vendor, complaints about subsequent commercial use of personal information by that vendor usually fail because the person "agreed" to that use as a condition of a purchase.[73] When a person complains that databases are being mined to identify her digital persona, a reductionist representation extracted from records of her purchases, uses and registrations, among other data, and that commercial solicitations focused on that digital persona are cluttering her physical and virtual mailboxes, those complaints usually fail because the data is not the person's property, but rather the property of the entity that collected it.[74] Analogously, when a person is physically present in a public space, he has limited grounds to complain if he is photographed there. The tort of false light protects against egregious misuse of a candid photograph, but courts consistently rule that such photographs can be used if there is a "legitimate connection" between the photograph and "a matter of public interest," a

[68] *Id*.

[69] *See* Smith v. Maryland, 442 U.S. 735, 743 (1979).

[70] *See* United States v. Miller, 425 U.S. 435, 442 (1976).

[71] The U.S. Congress subsequently passed laws that require judicial approval for police requests to telecommunication companies for the use of pen register and trap and trace devices and to banks for customer records; however, subpoenas suffice (rather than warrants) and the standard post 9/11 is relevance to a criminal investigation—a threshold that is easily crossed. *See* 18 U.S.C. §§ 3121–3127 (2006).

[72] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1148 (2002).

[73] VIKTOR MAYER-SCHONBERGGER, DELETE: THE VIRTUES OF FORGETTING IN A DIGITAL AGE (2009).

[74] Solove, *supra* note 72.

connection that is usually generously conceded.[75] Similarly, if a person drives a motor vehicle, he cannot complain if a police officer compares registration data for the license plate with a database of outstanding warrants.[76] Whatever value may be conceded to a person's private activities, those activities are vulnerable to third-party machinations whenever they stray across the private-public divide.

Some courts have attempted to apply a more nuanced view about privacy in instances where there has been a revelation of personal information to a limited audience. This idea of limited privacy—namely, that a person can reveal a private matter to a select group of persons and retain a legitimate expectation of privacy—has been upheld in the context of the tort of public disclosure of private facts.[77] In one case, a man who was HIV-positive told his friends, family, and a support group about his condition.[78] He agreed to appear on a local television show covering the positive effects of support groups after the station assured him that his face would be digitally blurred and that his identity would not be revealed.[79] The blurring was ineffective and members of the community recognized him.[80] The court opined that by limiting disclosure to persons with whom he had a close relationship, or who shared the condition, or were helping him cope with that condition, the plaintiff retained a reasonable expectation that his HIV-related information was private.[81]

Another case in which the court applied the concept of conditional disclosure involved a couple that conceived a child through *in vitro* fertilization.[82] Because their church opposed the practice of *in vitro* fertilization, the couple did not tell other people how they conceived their child; only hospital employees and one of their mothers knew about the procedure.[83] The couple was invited to a party sponsored by the hospital to celebrate its *in vitro* program's anniversary and the hospital "assured" the couple that there would be no public exposure of those attending the party.[84] However, reporters and a camera crew were present and, though the couple actively avoided the cameras, they were shown in a subsequent news story.[85] The court rejected the hospital's claim that because the couple attended the party with other couples, they had surrendered their right to privacy about their

[75] Delan by Delan v. CBS, Inc., 458 N.Y.S.2d 608, 613 (N.Y. App. Div. 1983).

[76] United States v. Ellison, 462 F.3d 557, 558 (6th Cir. 2006).

[77] Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d. 491, 500 (Ga. Ct. App. 1994).

[78] *Id*. at 494.

[79] *Id*.

[80] *Id*. at 493.

[81] *Id*. at 500.

[82] Y.G. v. Jewish Hosp. of St. Louis, 795 S.W.2d. 488 (Mo. Ct. App. 1990).

[83] *Id*. at 492.

[84] *Id*.

[85] *Id*.

participation in the program.[86] The court held instead that the couple "clearly chose to disclose their participation to only the other *in vitro* couples. By so attending this limited gathering, they did not waive their right to keep their condition and the process of *in vitro* private, in respect to the general public."[87]

Many jurisdictions have expressly rejected the idea of limited privacy for the public disclosure tort and otherwise, instead holding that once a person shares private information with another person, that person has waived the right to privacy about that information.[88] However, it is a mistake for our practices and laws to oversimplify the threshold between private and public. Instead, it is preferable to recognize degrees of public-ness. It is possible to re-conceive privacy protection in order to permit a person to function normally in a modern economy without unconditionally revealing public information in exchange for the necessities of life. The third-party doctrine need not encompass all records held by third parties, but instead might authorize or deny access depending upon the nature of the relationship between the parties and the expectations that arise from that relationship and the purposes served by disclosure. The revelation of public information need not be regarded as a surrender of the information to all who can access the information for all purposes. We can craft other thresholds for access and use of that information to serve the needs of private and governmental institutions to acquire and store personal information in order to authenticate individuals and access data about them where those uses are specified and limited in advance. This is an advance into the past because currently proposed limitations on use of personal information track recommendations articulated at the inception of technological changes that have privacy impacts. For example, a prescient response to the adoption of computer recordkeeping by the federal government recognized the potential for the cross-referencing of those records. A Code of Fair Information Practices prepared in 1973 for the then Department of Health, Education and Welfare (HEW) responded to worries about the growing computerization of federal government records by recommending that the law ought to provide a means "for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent."[89] This seemed a plausible policy of self-limitation to assuage fears of an overly powerful federal government, fueled by access to multiple records of its citizenry compiled by and for sundry federal programs.

Information technologies evolved rapidly and transformed the parameters of

[86] *Id*. at 502.

[87] *Id*. (distinguishing a legitimate public interest in an *in vitro* program from the identity of individuals participating in the program).

[88] Other jurisdictions have not adopted the third party doctrine. *See, e.g.*, State v. Hunt, 450 A.2d 952 (N.J. 1982); *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON 201 (2004).

[89] U.S. DEP'T OF HEALTH AND HUMAN SERVS., NO. (OS) 73-94, RECORDS, COMPUTERS AND RIGHTS OF CITIZENS 41 (1973).

the challenges addressed by the HEW Code. The private sector proved to be the more ambitious actor regarding information gathering and use.[90] Moreover, the pace of technological change has outstripped most efforts to manage its practices and impacts.[91] Existing categories for privacy protection were stretched to accommodate the growing challenges posed by the new technologies, and this strategy has mostly proven inadequate. At least part of the inadequacy is the reluctance to surrender simplicity for complexity, and to acknowledge the variability of privacy norms in different social settings and to devise appropriate means by which to evaluate the impact of technological change upon those norms.[92] Privacy concerns are easier to accommodate when they can be described along a single axis, as a single variable that is relevant in the same way in every context. When privacy is weighted differently in different contexts, with emphases that vary according to the particular characteristics of the parties and their norms and practices, the process of review is inevitably complicated. This increased complexity is a disincentive to adopt a perspective that recognizes that privacy is highly context dependent.[93]

Helen Nissenbaum has championed the idea that privacy protection should be re-conceptualized by adopting methodologies that are more context sensitive. She has articulated a framework for "contextual integrity" whose premise is that "finely calibrated systems of social norms, or rules, govern the flow of personal information in distinct social contexts . . . and define and sustain essential activities and key relationships and interests, protect people and groups against harm, and balance the distribution of power."[94] Nissenbaum has provided a method of evaluating "policy and regulation, court decisions and law, and technology design and implementation" that uses context-specific informational norms to determine "whether social-technical devices, systems, and practices affecting the flow of personal information in society are morally and politically legitimate."[95] This insistence upon the context sensitivity of privacy norms is currently a minority view, but it may prove ascendant. It is founded on well-developed schools of thought in sociology and philosophy that recognize the variability of norms according to

[90] ROBERT O'HARROW, JR., NO PLACE TO HIDE: BEHIND THE SCENES OF OUR EMERGING SURVEILLANCE SOCIETY (2006).

[91] Andrew Askland, *Introduction: Why Law and Ethics Need to Keep Pace with Emerging Technologies*, *in* THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT, xiii (Marchant et al. eds., 2011).

[92] JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000).

[93] Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L .REV. 1087 (2002).

[94] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 3 (2010).

[95] *Id*. at 7, 236.

their social setting.[96] The application of that approach to privacy, however it is defined, would deem privacy a norm that is expressed differently according to variations among parties and practices as they are affected by particular applications of invasive technologies.

V. TRIPLE TEAMING PRIVACY.

The limited legal response to invasions of privacy is at least partially the result of several recent and ongoing trends. First, courts have been reluctant to take a lead role in addressing technological change, especially when those changes are still in progress, deferring instead to the legislature.[97] This reluctance is pronounced in cases involving privacy, at least in part because of uncertainty about its weight or limits. Second, legislatures are overwhelmed by the pace of technological change and struggle to identify and balance the interests that are stake.[98] Those interests include the commercial gains derived from privacy invasive practices. Lobbyists representing commerce can realize concentrated benefits for their clients by imposing distributed costs upon an inattentive public.[99] And third, these trends are framed by security sensitivities that have not fully recovered from the shock of Al-Qaeda's attack upon the homeland. These several trends merit elaboration.

The terrorist attacks on September 11, 2001, and the subsequent War on Terror provided the rationale for enabling maximal access to databases and reducing privacy protection in the name of national security. These changes exploited the inter-accessibility of federal records to assist security focused programs and also, as privacy protection thresholds dropped, other uses that have apparent utility.[100] The use of records collected for one use to serve another use had been explored before 9/11, such as comparing lists of federal employees to records of people receiving benefits through Aid To Families with Dependent Children (Project Match) or recipients of federal benefits with lists of individuals with outstanding state and local child care arrearages.[101] Such uses were initially justified as "routine use" of the information to avoid coverage by the Privacy Act and later protected by legislation, namely the Computer Marketing and Privacy Protection Act.[102] The War on Terror

[96] TALCOTT PARSONS, THE SOCIAL SYSTEM (2d ed. 1991); DANIEL SPERBER, EXPLAINING CULTURE: A NATURALISTIC APPROACH (1996).

[97] Askland, *supra* note 91.

[98] *Id*.

[99] WILLIAM N. ESKRIDGE, JR., ET AL., LEGISLATION AND STATUTORY INTERPRETATION 83 (2d ed. 2006).

[100] FREDERICK A.O. SCHWARZ, JR., & AZIZ Z. HUQ, UNCHECKED AND UNBALANCED: PRESIDENTIAL POWER IN A TIME OF TERROR 127 (2007).

[101] PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 88 (1995).

[102] *See* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public*

expanded the reach of database comparisons, inspired the public sector to share its databases of personal information with government officials, and generally enabled private sector access to and use of personal information with minimal limitations.[103] The steady drumbeat of security concerns drowned the appeals of privacy advocates that security-justified practices were overreaching the boundaries of their rationales.[104] A reconsideration of security risks and effective means to address those risks can better focus our practices.[105] It is possible to enable a robust government response to the threat of terrorism without reducing privacy protection for assaults that are not justified by security concerns.

An entrepreneurial spirit that already discourages the adoption of protections that might thwart the generation of profit with innovative practices that mine databases for probative links to purchases, subscribers, contributors, etc., flourishes in the wake of reductions in privacy protection rationalized by a fear of terrorist acts. There is a well-worn pattern in legislative efforts to protect privacy to defer to the private sector's concerns about the impact of privacy protection upon their practices.[106] As a consequence of this piecemeal, interminably negotiated approach, there is no comprehensive vision of legislative privacy protection. Instead, there are nobly titled, but humbly phrased bills that ostensibly respond to the periodic privacy violations that manage to attraction public attention. The resulting statutes generally have a minimal impact upon practice and are sometimes so narrowly drafted that the abuses that they intend to curtail elude coverage because the objectionable practice, driven by rapid technological change, has mutated beyond the language of the statute. The Stored Communications Act, for example, distinguishes between electronic communications held in storage for 180 days or less and for more than 180 days.[107] A warrant supported by probable cause is required to access the former, but a subpoena and prior notice suffices for the latter.[108] This distinction between 180 days or less and more than 180 days was created before the ubiquity of the internet and email communication; in addition to misevaluating email stored in folders in contrast with undeleted

Sector Regulation in the United States, 80 IOWA L. REV. 553, 588 (1995); 5 U.S.C.§ 552 (2006).

[103] DAVID LYON, THE ELECTRONIC EYE: THE RISE OF THE SURVEILLANCE SOCIETY 78 (1994).

[104] Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 81 (2005).

[105] Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343 (2008).

[106] REGAN, *supra* note 101.

[107] Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2701–12 (2006)); *see* § 2703.

[108] 18 U.S.C. § 2703 (2006).

voice mail (which was the prevailing stored electronic communications at the time the Act was passed), it also ignores the role of Internet Service Providers (ISP) in the storage process, including the status of email held by an ISP before it is accessed by the account user.[109] The inadequacy of the Act's language and the disinclination to revise that language to accommodate changed facts is consistent with much federal legislation that is either written or vetted by lobbyists for organizations whose practices are affected by the bill.[110] The combination of overreaching security and over-protective profit seriously dilutes efforts to devise and implement a comprehensive privacy policy.

It is not only the War on Terror and the prerogatives of the market that promote maximal access to public records. The courts also narrowly construe and sometimes only reluctantly concede the right to privacy.[111] Moreover, the foundations for a right of privacy are spread across many sources that do not speak in a single voice. Privacy is legally grounded in constitutional law, tort law, and statutes. The United States Constitution and state constitutions support the right of privacy in several settings or "zones of privacy," but the strength of the protection depends upon the zone.[112] The zones where the right of privacy has been recognized are limited, arguably "to those which are 'fundamental' or 'implicit in the concept of ordered liberty.'"[113] Further, the right of privacy's growth has been slow, even among states courts where the state constitution specifically articulates a privacy right. As one court phrased it, "[a]lthough cases exploring the autonomy branch of the right of privacy are legion, the contours of the confidentiality branch are murky."[114] A number of privacy-related torts have been identified in various states' common law or established by legislative action, but the scope of these torts have been reduced by their friction with the First Amendment. For example, efforts to protect the identities of rape victims have often failed because they conflict with

[109] Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 322 (2011).

[110] *Id*. at 323.

[111] Tracy Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 58 (2002); Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1305 (2002).

[112] Justice Douglas introduced the term 'zones of privacy' into Supreme Court analyses of privacy claims in *Griswold v. Connecticut*, 381 U.S. 479 (1965), to describe subject areas where there is a constitutional right to privacy.

[113] Paul v. Davis, 424 U.S. 693, 713 (1976). *Paul* was decided before *Whalen v. Roe*, 429 U.S. 589 (1977), where the court appeared to endorse the appellee's contention that two constitutionally protected zones of privacy interests were at issue, in "avoiding disclosure of personal matters" and in "independence in making certain kinds of important decisions," though the court concluded that, given the facts before it, there was no constitutional violation. *Whalen*, 429 U.S. at 599–600.

[114] Scheetz v. Morning Call, Inc., 946 F.2d 202, 206 (3d Cir. 1991).

expansive views of newsworthiness.[115] Various federal and state statutes address practices that affect privacy and implicitly create privacy rights, but, as noted, these statutes are usually narrowly phrased to address specific abuses and often fail to achieve even these limited purposes.[116]

There is no coordinated statement of the force and limits of privacy rights, and courts have ranged across a spectrum of responses to the resulting ambiguity. Most courts err on the side of caution, especially when faced with novel fact settings, unclear precedent, and insufficient legislative guidance. One court expressed "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information" in its review of the "Delphic" guidance provided by relevant Supreme Court holdings.[117] A narrow construction means that privacy complaints are easily dismissed as inapposite or diminished as insufficiently weighty when offered to resist privacy invasive practices.[118] Because privacy's status as a right is generally limited to very specific applications, it is often regarded as an interest to be balanced against other contending interests. It is difficult to generate consensus views about the monetary value of privacy, and thus privacy usually loses in cost/benefit analyses where the cash value of a privacy-invasive practice can be demonstrated with familiar market terms and evidence. For example, the federal legislative determination that an opt-out provision for the sharing of personal data by financial institutions was more reasonable than an opt-in provision relied upon a comparison of the cost and inconvenience to the affected industry, which was substantial (because the consent of individual consumers would be required before sharing of their information could occur), against the inconvenience to the individual consumer, which was adjudged minor.[119] This approach to calculating costs and benefits will generally favor commercial interests that can specify their benefits and disfavor consumers whose costs are individually small. The accumulation of many affected

[115] *See* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 475 (1975); Florida Star v. B.J.F., 491 U.S. 524, 532 (1989).

[116] *See, e.g.*, Driver's Privacy Protection Act, 18 U.S.C. §§ 2721–2725 (2006) (restricting the disclosure of information in state motor vehicle records, while other state records are unaddressed by federal law); Video Privacy Protection Act, 18 U.S.C. §§ 2710–2711 (2006) (prohibiting the disclosure of videotape rental information by video stores, but does not address similar disclosures by bookstores, record stores, retail sales companies); Telephone Consumer Protection Act, 47 U.S.C. § 227 (2006) (providing remedies for recent telephone calls from telemarketers, but does not address access to the telephone numbers of consumers).

[117] Am. Fed'n of Gov't Emp. v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997).

[118] Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or a Frontier for Individual Rights?*, 44 FED. COMM. L.J. 195, 209 (1992).

[119] Mainstream Mktg. Servs., Inc., v. FTC, 358 F.3d. 1228 (10th Cir. 2004).

consumers who bear the transaction costs[120] and the general diminution of privacy expectations will likely be deemed insufficient to outweigh the costs (or reduced profits) to industry.

VI. A POSSIBLE FUTURE FOR PHOTO RADAR TECHNOLOGIES.

There are profound reasons to be wary of a renewal of extensive photo radar enforcement. The renewal would arise in a social and legal culture that provides diminishing protection for privacy and would focus on motor vehicle transportation, an area that is already heavily regulated. If cost effectiveness is the primary constraint on the practice, then improvements in the underlying technologies and reductions in their cost may invite a future wide scale use of photo radar. If cost effectiveness is combined with perceived improvements in safety, then the placement of photo radar may expand to cover all streets within specifically classified areas, such as areas with high pedestrian use or the presence of young or vulnerable populations. The expansion might easily entail multiple devices on high priority streets and a generous definition of boundaries for qualification as a classified zone. Photo radar enforcement might become an expression of neighborhood empowerment, a step up from speed bumps, stops signs, and rotary traffic circles. Photo radar enforcement might eventually encompass all streets located where residents are actively protective of neighborhood safety, and the looming ubiquity of the devices might challenge the delimitation of a qualifying offense. For example, for what distance need an individual drive a vehicle at an illegal speed to qualify for more than one speeding citation? Perhaps one citation per city block is a reasonable compromise for determining the liability of speeding motorists and might serve as a limit on the number of devices per block. Otherwise, if photo radar devices become as inexpensive as closed circuit television (CCTV), devices might be positioned on every light pole on every street.

This exaggerated expansion of photo radar enforcement portends elaborations of an already available alternative means of enforcing speed limits. Some rental vehicles are currently outfitted with Global Positioning System (GPS) equipment that enables the tracking of the use of the rental vehicle and the violations of applicable traffic laws during that use.[121] Many trucking companies have adopted GPS systems to track the whereabouts and use of their vehicles.[122] A later elaboration might be GPS for all registered

---

[120] *See* Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

[121] Anita Ramasastry, *Tracking Every Move You Make: Can Car Rental Companies Use Technology to Monitor Our Driving? A Connecticut Court's Ruling Highlights an Important Question*, FINDLAW.COM (Aug. 23, 2005), http://writ.news.findlaw.com/ramasastry/20050823.html.

[122] Erik Eckholm, *Private Snoops Find GPS Trail Legal to Follow*, N. Y. TIMES, Jan. 29, 2012, at A1.

vehicles and a monthly report of violations of traffic laws as identified by GPS monitoring, perhaps coordinated with the vehicles' Event Data Recorder.[123] We have already seen the adoption of GPS technologies for cell phones and many motor vehicle manufacturers offer GPS devices for their products. Auto loans or insurance coverage might be conditioned on access to GPS data or, less coercively, reduced rates might be offered as an inducement to the accept GPS monitoring. The insinuation of the technology into everyday life and its reduced cost will facilitate expanded future use of GPS. Pushing a little harder, the step beyond GPS for motor vehicles may be throttle controls that are activated by GPS so that motor vehicles cannot exceed speed limits because their engine governors will not let them.

There are also other kinds of motor vehicle monitoring. Automatic number plate recognition (ANPR) systems are in operation in the United Kingdom.[124] This system is comprised of a network of cameras, located at fixed locations and on police vehicles, which can detect and record license plate numbers on vehicles using the national highway system.[125] Though it is largely a sequence of snap photographs, it is capable of tracking the movement of individual vehicles.[126] In the United States, radio frequency identification (RFID) technology is used for many purposes, including the enabling of E-ZPass toll highways.[127] A transponder tag in enrolled vehicles permits the E-ZPass system to directly bill toll fees to the enrolled driver's account.[128] The system could also identify speeding violations when there is more than one toll plaza and multiple receivers compare distance and time to compute speed.[129] Finally, the U.S. Department of Transportation is studying a proposal to equip every motor vehicle with a device that would permit comprehensive monitoring of vehicles in operation on specific roadways in order to identify and report roadway conditions such as congestion, accidents, hazardous conditions, etc.[130] Potentially, all vehicles could be monitored at all times. It

[123] Andrew Askland, *The Double Edged Sword That Is the Event Data Recorder*, 25 TEMP. ENVTL. L. & TECH. J. 1, 11 (2006).

[124] Ray Massey, *Drivers Can Avoid Speeding Tickets . . . by Changing Lanes*, DAILY MAIL (London), Oct. 15, 2006, http://www.dailymail.co.uk/news/article-410539/Drivers-avoid-speeding-tickets--changing-lanes.html.

[125] *Id.*

[126] *Id.*

[127] Chris Newmarker, *Attention Cheaters: E-ZPass is Watching You*, DAILY NEWS (New York), Aug. 10, 2007, http://www.nydailynews.com/news/attention-cheaters-e-z-pass-watching-article-1.236001.

[128] *Id.*

[129] *See id.* (noting that toll information has been used in other circumstances to track drivers).

[130] Michael Cooney, *U.S. Wants to Build Cybersecurity Protection Plan for Cars*, NETWORK WORLD (Aug. 3, 2011), http://www.networkworld.com/community/blog/us-

may be the case that safety, especially safety linked to national security, trumps all contending counter considerations, and even tangential allusions to its talismanic powers evokes a dispositive argumentative force.

It may be a poor argument strategy to tie personal freedom to the medium of a motor vehicle. The operation of a motor vehicle is "subject to pervasive and continuing government regulation and control."[131] Increased regulation in the future is likely. There are already substantive environmental and resource pressures that affect the design and capacities of motor vehicles. Safety concerns as expressed in efforts to effectively restrain violations of applicable speed limits may be reasonable extensions of a growing societal need to regulate the design and operation of motor vehicles. The future of motor vehicle use will likely be considerably more managed than is now the case. Vehicles may be 'freed' from individual driver handling and instead largely controlled by external computers which can better coordinate access to and use of public roadways. Perhaps the future will entail a few moments of programming one's vehicle and the subsequent submission to an automated course of travel, both route and speed, that avoids the idiosyncrasies and limitations of individual drivers.

Regardless of the accuracy of these speculations about future roadway use, there are different pathways forward, and at least some of them recognize the impacts that a new technology may have upon personal privacy and attempts to accommodate the value of privacy. "The physical characteristics of an automobile and its use result in a lessened expectation of privacy,"[132] but less need not mean none. Ignorance of the impacts that new technology has on privacy plays out as an unconditioned deferral to the prerogatives of that particular technology. It also reinforces a broader public insensitivity about the trade-offs between privacy and privacy-invasive technologies. Changes to how we transport ourselves in motor vehicles or their successor technologies are inevitable, but the form of that change is negotiable; it can be phrased to respect privacy, for example as a "return to the task of preserving the environment that makes privacy possible,"[133] or it can advance indifferent to its effects upon privacy.

It is the prospect for an unchecked expansion that forms the basis of this Article's privacy-based objections to photo radar. A practice initially justified by its safety impacts may change over time to provide diminishing safety benefits even as it further squashes an important zone for privacy protection.

---

wants-build-cybersecurity-protection-plan-.

[131] South Dakota v. Opperman, 428 U.S. 364, 368 (1976).

[132] New York v. Class, 475 U.S. 106, 112 (1986); *see* Cardwell v. Lewis, 417 U.S. 583, 590 (1974).

[133] Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1481 (2004).

Photo radar located where a history of observations justifies safety concerns may be extended to photo radar whose benefits are more tenuously evaluated, either in individual locations or for its systematic effects as it encompasses all driving. What initially appears to be a focused enforcement effort may expand to comprehensive proportions, making the operation of a motor vehicle into a wholly-monitored activity.

We have apparently acquiesced to the determination that photo radar enforcement of traffic laws is a justified imposition upon privacy,[134] at least when pursued at a modest level. It need not be the case that this decision commits us to approve of widespread photo radar enforcement. The two approaches are distinguishable and that distinction is better realized when each is evaluated separately. We can identify a different balance of interests in the two contrasting applications. It is important not to presume that the acceptance of the lesser imposition is an acceptance of the larger imposition. It appears that there has been a recent hesitation between modest use and widespread use. The hesitation provides a propitious moment to articulate the reasons why we should refrain from adopting widespread photo radar enforcement in the future.

It is preferable to highlight the distinction in order to retain privacy rather than to identify and recover it later. Recoveries of lost privacy can be accomplished: witness the recent Supreme Court decision regarding GPS devices attached to motor vehicles without the authority of a warrant.[135] Police practice evolved from physically trailing a vehicle to inveigling a beeper into property transported in the trailed vehicle[136] to attaching a GPS device to the trailed vehicle without a warrant, an escalation of enhanced surveillance without Fourth Amendment protection until the Supreme Court declared that the GPS placement required a warrant.[137] One might ponder how GPS placement on a vehicle by police could escape the Fourth Amendment, but clearly reasonable people were persuaded by the gradual accumulation of practice to conclude that it was not covered. Fourth Amendment protection for situations involving motor vehicles has been shrinking with each passing case scenario, and it might seem that the Fourth Amendment has no application, rather than a heavily constrained one.

It is preferable that we adhere to the judgment that widespread photo radar is an offensive imposition upon our privacy and limit the weight of police surveillance to isolated applications of photo radar that are justified by a record of danger and harm. The operation of a motor vehicle exposes drivers to considerable police scrutiny when it is reasonably related to public safety.

---

[134] Agomo v. Fenty, 916 A.2d 181, 190 (D.C. 2007) ("[A]lthough cameras operated by the Government created a privacy issue, those concerns were outweighed by the legitimate concern for safety on our public streets.").

[135] United States v. Jones, 132 S. Ct. 945 (2012).

[136] United States v. Knotts, 460 U.S. 276 (1983).

[137] *Jones*, 132 S. Ct. 945.

That exposure need not be unlimited and one may maintain an expectation of privacy while operating a motor vehicle that is consistent with the recognition of appropriate police powers.

CONCLUSION

Roadway safety is an important priority for state action and photo radar can be deployed to promote that vital exercise of police powers. However, there is a difference between targeted enforcement and ubiquitous use of photo radar. Widespread use of photo radar reorients the balance between citizens and their government by broadly empowering government to impose upon the privacy of its citizens. The expansion of government power is partly the result of improved technologies that enable heightened surveillance of citizen activities, on the road and elsewhere. Indeed, technological advances have transformed the methodologies of law enforcement so that investigations need not focus on discrete evidence to identify suspects, but instead can reference databases of various kinds to cull out individuals with statistically relevant characteristics. Targeted enforcement, on the other hand, better comports with a conception of the reasonable expectation of privacy that attempts to balance vital social and individual interests. Resistance to widespread use of photo radar is an opportunity to eschew technological changes simply because they are available, and, more importantly, to reconfigure the balance between citizens and their government, insisting upon less privacy-invasive practices.