Photo Radar Enforcement as a Slippery Slope

Andrew Askland, Arizona State University

Available at: http://works.bepress.com/andrew_askland/2/
Photo Radar Enforcement as a Slippery Slope

Enforcing speed limits for motor vehicles with photo radar is widely practiced throughout the United States. The Dutch company Gatsometer BV introduced the speed camera in 1964, the incidental product of a rally driver’s efforts to accurately monitor his speed on a racetrack. The technology evolved to red light cameras in 1965 and to roadway traffic speed cameras in 1971.\(^1\) The use of photo radar increased dramatically when digital cameras were introduced in the 1990s. Driven by pressure (including state constitutional mandates) to reduce large state budget deficits, photo radar enforcement bubbled expansively between 2008 and 2010 after which use subsided to pre-surge levels. The surge can be traced to several factors, but third-party contractors who offered to install and manage photo radar equipment and promised revenue windfalls are an important part of the explanation.

As an example, photo radar enforcement of speeding laws was adopted as a state-wide program in Arizona in October, 2008 with some trepidation among government officials about public response. The program was terminated less than two years later, in July, 2010.\(^2\) The program’s sponsors acknowledged that its primary purpose was to generate revenue to close an unprecedented budget revenue shortfall. The program was authorized by changes in the governing Arizona statute which provided in part that speeding citations issued pursuant to the newly instituted program would not be considered a violation for the purposes of license revocation or suspension, \textit{i.e.}, no points were assessed for violations. The program was discontinued at the level of state enforcement via the third party contractor (Redflex Traffic Systems) when the original contract expired, but there remain roughly 14 municipal photo radar programs within the state and, 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.\(^3\) Like the situation in Arizona, the country-wide downturn in the use of photo radar can be attributed to several concerns about its expanded use: third-party delegation of police powers;

\(^{1}\)Http://www.gatsometer.com/.


enforcement fairness; service of process complications; negative public response; and revenue disappointments.

This paper will first survey several recurring criticisms of wide-spread photo radar enforcement and identify likely changes in practice that might defuse those criticisms. The paper will then briefly examine the private-public dichotomy that dominates legal analysis of how to respond when private matters are exposed to public view. Three factors strongly influence the response and diminish the protections afforded to privacy. These factors are 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. The paper closes with some speculations about future use of photo radar enforcement and other motor vehicle-focused surveillance technologies.

Problems with Widespread Photo Radar

The delegation of law enforcement to third-party contractors was objectionable on several grounds. The training and supervision of individuals who operate the programs were outsourced to third-party contractors who were not directly answerable to elected officials as are police personnel. The attenuation of the chain of responsibility is problematic because it shelters actors performing police power functions behind contractual provisions that were 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 their policies are shaped by that motivation 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 the benefits are so obviously tied to volume. One court, addressing photo enforcement of red light violations, stated that the
“conflict of interest created by a contingent method of compensation . . . undermines the trustworthiness of the evidence.” 4

The challenge of linking driver photographs to data for the vehicle’s registered owner prompted widespread unfairness complaints about enforcement because, e.g., 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 (in some cases with masks) when the enforcement photograph was taken were not ticketed; vehicles with dirty license plates or plate covers were not ticketed; etc. 5 Inconvenience and expense largely explain these failures to pursue enforcement, but from the perspective of fairness and equity, these justifications may appear objectionably arbitrary. If speeding is the focus of concern, then a concerted effort to identify and prosecute speeders should attempt to overcome these obstacles to a comprehensive and thereby more effective enforcement.

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. 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. These fairness complaints provide fodder for public dissatisfaction with photo radar enforcement programs, but they are likely insufficient to support an equal protection or a due process challenge to particular programs. Nor has the privacy interest at stake been identified as a fundamental right to qualify for subjective due process protection. The state’s compelling

5 Arizona estimated that 47 per cent of its photographs were rejected during the first year of its state wide program. Report of the Arizona Auditor General on the Department of Public Safety Photo Enforcement Program, January 19, 2010.
interest in roadway safety likely overcomes these shortcomings in the implementation of the programs.\(^6\)

An additional potential problem with photo radar is service of process issues. Service of process to photographed drivers proved problematic and expensive as courts sometimes would not accept first class mail delivery of citations as adequate service.\(^7\) 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.\(^8\) Prosecutors were 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. 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 obligating a registered motor vehicle owner to report the identity of the vehicle operator when a violation occurs or otherwise 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 not ready to rely upon other legal or policy arguments that had not yet congealed as judicially recognizable or dispositive.\(^9\)

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

\(^8\) People v. Hildebrandt, 126 N.E. 2d. 377 (NY 1955), is the first case where a court refused to accept a presumption that the owner of a vehicle is the operator of that vehicle when a device detects a violation.
\(^9\) One expression of judicial qualms about photo enforcement is a decision of a California appellate court that required 30 days notice at each intersection with a red light camera before the camera was activated.
public has generally voted against the programs. Photo radar programs have been proposed to
the electorate as a referendum issue in various localities and were rejected in Peoria, Arizona;
Batavia, Illinois; Steubenville, Ohio; Anchorage, Alaska; and Sykesville, Ohio; *inter alia.*

Complaints about the programs are not limited to violators, but also arise 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.10 The photographs
present a special concern because they make drivers unwilling subjects of public scrutiny. For
this particular privacy invasive technology, the rising surveillance society 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.11 State budgets were in peril in
the aftermath of the mortgage banking industry collapse, but the crisis mode passed. Anticipated
revenue enhancements were more carefully reviewed as the crisis was averted and relevant data
came available. Given that the abrupt increase in use of photo radar was rationalized by
substantial projected revenue increases, when the projections proved unduly optimistic, a
primary rationale for the surge in photo radar use failed.

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, *e.g.*, 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).
Photo radar is still used to enforce speed limits, but the enforcement has largely reverted to
police control and it no longer aims to identify a maximal number of violators in order to
significantly supplement income for local and state coffers.

**Defusing Widespread Photo Radar Problems**

---

8, 2010.
The dampening of the enthusiasm for widespread photo radar enforcement programs may not be permanent. There is no guarantee that widespread photo radar enforcement will not be reintroduced at a later time, perhaps when some 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. An emphasis upon increased safety rather than increased revenue as a justification for photo radar (and the placement of photo radar informed by safety rather than revenue considerations) would likely make it more palatable. Photo enforcement might be touted as a means to remove the potential bias of the individual police officers who issue citations. Various photo 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. 12

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.

The imposition upon registered motor vehicle owners arguably constitutes a 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

12 For example, the Rockville City Police in Montgomery County, Maryland, e.g., highlights its hiring of new police officers “solely dedicated to traffic enforcement” in its assessment evaluation of its photo radar speed enforcement. Safe Speed Program Evaluation, released July 23, 2009.
Driving is regarded as a privilege rather than a right and the privilege can be conditioned by the state so long as the conditions are reasonable. In an era that is haunted by terrorism threats and succumbs to progressively more invasive surveillance technologies, the plasticity of a reasonableness standard might accommodate these “driver liability” or “tattle or pay” impositions upon vehicle registration. Drivers are required to maintain a current mailing address with the motor vehicle administration to receive notices relating to their licenses, e.g., renewals, proposed suspensions, etc., and owners are similarly required to maintain that information for vehicle registration renewals. First-class mail is generally deemed adequate notice for these purposes. The use of first-class mail is already the current practice in Canada and in some states for traffic violations. Appellate courts might well view a legislatively imposed burden to report on illegal vehicle use to be reasonable.

A Problem of Over-Inclusiveness

The prospect of expansion of 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, specifically what monitoring of their behavior is reasonable. Law enforcement has costs and 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. 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.

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, i.e.*, wrongful not on account of an intrinsic quality (a natural evil), but only because of statutory or regulatory stipulations.

We may not want to enforce all laws in all instances 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 what is the focus of concern from what is technically a violation, but not intended to be covered. 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 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. We may also negatively affect the public perception of drunk and disorderly statutes as appropriate remedies for problems that are inexactstly 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 law breaker. Continual monitoring of public streets might provide evidence of technical violations that would undermine confidence in the governing statute and in law enforcement generally.

The Private – Public Dichotomy

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 it 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,” or tests offered as alternatives to Katz when such 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 a fully visually monitored activity. Operating a motor vehicle ceases to be the movements of a presumably privacy protective person than the maximally monitored activities of a member of a suspect class, as though a convicted criminal (perhaps as a probationer) who has forfeited civil rights on account of prior grievously wrongful conduct. (Beware Jeremy Bentham’s Panopticon!) Whatever the merits or demerits of photo radar enforcement that is solely focused on historically problematic stretches of roadway, the unchecked expansion of its use portends qualitatively different challenges that significantly and objectionably burden 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.

The all-or-nothing approach that is promoted with a mechanical enforcement of law tracks a general inadequacy in phrasing protections for privacy. Clarity, predictability and ease of administration argue for sharp distinctions, but complex problems are often ill-suited to simple solutions. Despite periodic dissent, e.g., 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,” or Justice Stevens’ acknowledgement 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,” 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

16 Jeremy Bentham, Panopticon: The Inspection House (1787). 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 is explored in Michel Foucault, Discipline and Punish: The Birth of the Prison (Random House, 1975).
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” and the threshold determination that something is public is usually regarded as non-problematic. Once a private matter becomes public, and the dividing line is perceived to be fairly sharp, use of that previously private matter is largely unconstrained. The sharpness of the boundary makes the distinction easier to enforce, thereby promoting judicial economy, but it does not necessarily comport with widely shared expectations about when behavior qualifies as public (and advances in information technologies and social media are rapidly exposing these disappointed expectations, e.g., 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 that the citizen required the repose of a private household to succor his mental strength and restore his spiritual equilibrium. 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.

This dichotomy has been the source of feminist criticism because it can shelter abuses within the family from public scrutiny, e.g., the physical abuse of wives by husbands was ignored by courts that declined to interfere in private family matters. Despite the misuse, the public-private distinction is useful when it is better explicated and more carefully 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

---

19 Melvin v. Reid, 297 P. 91 (Cal 1931).
21 State v. Rhodes, 1868 WL 1278 (1868).
community and culture to define herself.\textsuperscript{22} 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 \textit{and} public; it is folly to expect a sharp boundary marking where they cross 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 can be squeezed by a draconian, omnipresent surveillance or overindulged in hyper-insulated isolation. Privacy should not be reduced to unexpressed thoughts, but instead must include stages of expression that stretch from diary entries and confidential conversations to disclosures within a support group and internet mediated purchases of consumer goods.

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 multiple contexts (\textit{e.g.}, police access without a court order to records maintained by phone companies\textsuperscript{23} and banks\textsuperscript{24}) that Fourth Amendment protections against search and seizure do not encompass records that a person voluntarily turns over to a third party.\textsuperscript{25} The effects of the third-party doctrine are harsh given that our contemporary lifestyles rely upon services provided by third parties, \textit{e.g.}, banks, merchants, credit card companies, public service utilities, etc.

The third-party doctrine reflects prevailing views about personal information that is held by third parties. If you provide information to a vendor, your complaints about subsequent commercial use of your personal information by that vendor usually fail because you “agreed” to that use as a condition of a purchase. If information about you is held in a database, your

\textsuperscript{23} Smith v. Maryland, supra.
\textsuperscript{25} 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.
complaints when that database is mined for commercial purposes to direct solicitations to you based upon the digital persona extracted from your record of purchases, uses, registrations, etc, usually fail because the datum is not your property, but rather the property of the entity that collected it.\textsuperscript{26} When you are physically present in a public space, you have limited grounds to complain if you are 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 connection that is usually generously conceded.\textsuperscript{27} If you drive a motor vehicle, you cannot complain if a police officer compares registration data for the license plate with a database of outstanding warrants.\textsuperscript{28} 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, viz, 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.\textsuperscript{29} In one case, a man who was HIV-positive told his friends, family, and a support group about his condition. 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. The blurring was ineffective and members of the community recognized him. 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 HI-related information was private.

Another case involved a couple who conceived a child through in-vitro fertilization. Because the practice was opposed by their church, the couple did not tell other people how they

\textsuperscript{26} Daniel Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. Cal. L. Rev. 1083 (2002).
\textsuperscript{28} U.S. v. Ellison, 462 F. 3d. 557 (6th Cir. 2006).
\textsuperscript{29} Multimedia WMAZ, Inc. v. Kubach, 443 S.E. 2d. 49 (Ga. 1994).
conceived their child; only hospital employees and one mother knew about the procedure. 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. However, reporters and a camera crew were present and, though the couple actively avoided the cameras, they were shown in a subsequent news story. 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 participation in the program. 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.”

Many jurisdictions have expressly rejected the idea of limited privacy for the public disclosure tort and otherwise, instead holding that once you share private information with another person, you have waived your right to privacy about that information. However, it is a mistake for our practices and laws to oversimplify the threshold for private to public. Instead, it is preferable to recognize degrees of publicness. 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 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

---

30 Y.G. & L.G. v. Jewish Hospital of St. Louis, 795 S.W. 2d. 488 (Mo. App. 488), distinguished a legitimate public interest in an in-vitro program from the identity of individuals participating in the program.
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.” The Code 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.

**Triple Teaming Privacy**

The shock of terrorist attacks on September 11, 2001 and the subsequent War on Terror provided the rationale for maximally enabling access to databases and other reductions in 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. The use of records collected for one use to serve another use had been explored before 9/11, e.g., 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. 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. The War on Terror 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. The steady drum beat of security concerns drowned the appeals of privacy advocates that security-justified practices were overreaching the boundaries of their rationales. A reconsideration of security risks and effective means to address those risks can better focus our practices. 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. 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 attract public attention. The resultant 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 or for more than 180 days. A warrant supported by probable cause is required to access the former, but a subpoena and prior notice suffices for the latter. 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 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, e.g., the status of email held by an ISP before it is accessed by the account user. 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.33 The combination of overreaching security and overprotective 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.\textsuperscript{34} 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 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. The zones where the right has been recognized are limited (arguably “to those which are ‘fundamental’ or ‘implicit in the concept of ordered liberty’”\textsuperscript{35}) and the right’s growth has been slow, even among states courts where the state constitution specifically denominates 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.”\textsuperscript{36} 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. Efforts to protect the identities of rape victims, for example, have often failed because they conflict with expansive views of newsworthiness.\textsuperscript{37} 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.

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.\textsuperscript{38} A narrow construction means that privacy complaints are easily dismissed as inapposite or diminished as insufficiently weighty

\textsuperscript{34} Tracy Maclin, Katz, Kyllo and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century, 72 Miss. L. J. 51 (2002); Ric Simmons, From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies, 53 Hastings L. J. 1303 (2002).

\textsuperscript{35} Paul v. Davis, 424 U.S. 693 (1976). Paul was decided before Whalen v. Roe and various commentators argue that the latter may provide for a broader recognition of judicially protected privacy rights, though not all commentators or courts agree with this interpretation.


when offered to resist privacy invasive practices. Because its 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 it 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 costs 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.39 Neither the accumulation of many affected consumers who bear the transaction costs 40 nor the general diminution of privacy expectations was sufficient to outweigh the costs (or reduced profits) to industry.

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, e.g., 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 in ‘civic minded’ neighborhoods and the looming ubiquity of the devices might challenge the

40 Jeff Sovern, Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information, 74 Wash. L. Rev. 1033 (1999),
delimitation of a qualifying offense, viz., for what distance need a vehicle be driven at an illegal speed for the driver 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. Many trucking companies have adopted GPS systems to track the whereabouts and use of their vehicles. A later elaboration might be GPS for all registered vehicles and a monthly report of violations of traffic laws as identified by GPS monitoring, perhaps coordinated with the vehicles’ Event Data Recorder.\(^{41}\) 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. It may be the case that safety, especially safety linked to national security, has trumping power across the board of 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.”\(^{42}\) Increased regulation in the future is likely. There are already substantive environmental and resource pressures that affect the design and capacities of motor

\(^{42}\) South Dakota v. Opperman, 428 U.S. 364 ( ).

18
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 and vehicles may be ‘freed’ from individual driver handling and instead largely controlled by external computers to better coordinate access 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 idiosyncracies 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” but less need not mean none. An ignorance of the privacy impacts of new technologies 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, i.e., a “return to the task of preserving the environment that makes privacy possible,” or it can advance indifferent to its effects upon privacy.

It is the prospect for an unchecked expansion that forms the basis of this paper’s privacy based objections to photo radar. A practice that is initially justified by its safety impacts may grow over time to provide diminishing safety benefits even as it further squashes an important zone for privacy protection. 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,\textsuperscript{45} 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 to decline 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 it 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. Police practice evolved from physically trailing a vehicle to inveigling a beeper into property transported in the trailed vehicle\textsuperscript{46} 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. 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

\textsuperscript{45}Agmo v. Williams, affirming Agmo v. Fenty, 2007 D.C. App. Lexis 11 (Feb. 1, 2007) held, in the context of red light photo radar, that "Although cameras operated by the government are a concern regarding privacy issues, those concerns are outweighed by the legislative concern for safety on our public streets."

safety. 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.