The Freedom of Information Versus the Right to Privacy

A Pro-Market Framework for Arizona

By
Solveig Singleton
Senior Analyst
Competitive Enterprise Institute

Arizona Issue Analysis 171
May 24, 2002
www.goldwaterinstitute.org

Executive Summary

The free movement of information throughout the economy and in government benefits Arizonans as citizens and consumers. At the same time, the right to privacy is also an important aspect of public and commercial life. Developments in information technology increasingly bring the free movement of information into conflict with the right to privacy.

Consider court records. Proponents of public access argue that the existence of open records is a cornerstone of the Anglo-American legal system. Opponents argue that bulk data processing gives the public too much access to private information. How should Arizona's policymakers decide between those competing principles?

This paper offers a general framework for balancing the interests between the free movement of information and the right to privacy and shows how that framework should be applied to address several pressing privacy questions in Arizona:

- Should red-light cameras be abolished in the interest of citizen privacy?
- Should court records and other public records be open to public scrutiny?
- Should legislators require websites to give visitors opportunities to opt out of or opt into information-sharing arrangements?
- Should the state of Arizona prevent websites from making good-faith changes in their privacy policies?

In summary, this paper finds that both the United States and Arizona constitutions protect citizens' rights to privacy vis-à-vis government intrusions, and those safeguards should be maintained. By contrast, the private sector should be free to use and transfer information about consumers for legitimate business purposes such as marketing or product development. Any new laws affecting the private sector should carefully target proven problem areas, such as credit card fraud, and the brunt of the law should fall on the criminals in question, not on legal businesses.

With regard to the privacy questions posed above, this paper comes to the following conclusions:

? *Red-Light Cameras.* Cameras in public places threaten privacy and due process and should be used as only a last resort. But the privacy impact of red-light cameras can be minimized with certain safeguards.

? *Court Records Accessibility.* Arizona should preserve access to public records for a broad range of legal purposes, from political activity to marketing to assessing credit risks. Blocking access to social security numbers in court records would do more harm than good, except perhaps for records open to casual onlookers over the Internet.

? *Consumer Privacy.* Broad state regulation of Internet or consumer privacy, whether of an opt-out or opt-in nature, is not needed and would harm Arizona consumers and businesses, both large and small.

? *Privacy Policies on the Internet.* Businesses that conduct electronic commerce need flexibility to draft, and sometimes redraft, their privacy policies, as they do with any other contract term.

Key Questions about Privacy Policy in Arizona

As more Arizonans join the web culture, and as technology transforms more aspects of our lives, anxiety has grown regarding several privacy issues:

- ? Should red-light cameras be abolished in the interest of citizen privacy?
- ? Should court records and other public records be open to public scrutiny?
- ? Should Arizona force websites to provide visitors with an opportunity to opt out of or opt into information-sharing arrangements?
- ? Should the state of Arizona prevent websites from making good-faith changes in their privacy policies?

Basic Principles: Balancing Privacy and the Freedom of Information

There has always been tension between privacy and free expression. Journalists may investigate and write about the subjects of news stories without asking the subject's permission. Banks report our late or timely loan payments to credit reporting agencies, so that merchants will sell goods to consumers on credit. This free exchange of information has many benefits. But the law also recognizes the need for privacy. Doctors recognize that they must protect the confidentiality of medical records, or their patients will no longer be forthcoming about sensitive medical problems. And none of us want to live in a society where Big Brother stamps out dissent by constant surveillance.

What principles can we use to make sense of these conflicting interests? Seeking information about others is natural behavior. For neighbors, coworkers, and friends, the normal rule of human relationships is that people are free to learn and talk about other people. The same is true in business. Websites are no different—indeed, their need to learn about their visitors is even greater, because over the Internet we are all strangers dealing with strangers. The general principle, simply stated, is that human beings in a free society should be free to learn about each other and exchange that information, as long as others' property or contract rights are not violated. This is true with regard to journalism, credit reporting, or ordinary gossip. In exceptional circumstances, such as in the practice of law or medicine, the rule is reversed, so that lawyers or doctors have an obligation to protect privacy. Freedom of information has been the rule, with legal obligations protecting privacy the exception.

Although information is also important to the government, the collection of information by government presents special problems. Governments have powers that the private sector lacks, such as the authority to control the police and the courts. Both the U.S. and Arizona constitutions protect privacy in order to prevent those government powers from being abused. But the constitutional guarantees of privacy do not, and should not, apply to the private sector.

Red-Light Cameras

Arizona is one of several states in which red-light cameras have been used to control the serious problem of drivers running red lights frequently at certain intersections. In 2001, the Institute of Highway Safety published a study showing that Phoenix, Arizona, ranked first in the country for red-light crashes, with Mesa, Arizona, ranking third.[1]

Around the United States, red-light cameras and other public surveillance technologies have generated a tremendous amount of unease among privacy advocates and the general public. Such public video surveillance is disturbingly reminiscent of George Orwell's vision of the world of Big Brother. Noted advocates of limited government such as Dick Armey have opposed the use of such cameras.[2] Can the concerns of limited government be reconciled with the use of red- light cameras?

Constitutional Principles

According to the basic principles described in the introduction to this paper, any surveillance by government is uniquely susceptible to abuse and is therefore limited by familiar constitutional principles. But no constitutional privacy principle bars police surveillance of people's activities in public places, and the intersection of a street is certainly a public place. A red-light camera in a public place can be a cost-effective substitute for hiring a police officer to stand there. In this sense, red-light cameras do not violate traditional privacy principles (as opposed to due process concerns). Indeed, in a sense the red-light camera is less intrusive than the constant presence of an officer. An officer would observe all the traffic going by. Usually, the red light camera is triggered *only* by red light violators.

The main constitutional problem with red light cameras may not be that they observe too much, but that their observations produce information that is too poor to satisfy due-process requirements. If the red-light camera is trained only on the license plate, the photograph cannot establish who is driving the car. The state should not assume the guilt of the car's registered owner. Consistent with this, Arizona law nullifies the ticket if the view of the driver's face is obstructed.[3] The cameras also may ticket those who have been trapped in the intersection by slow-moving cars ahead, who are not necessarily "running" the red light, or those who brake to a stop just past the white "stop" line. Many photographs show only a partial or unclear license plate. To protect due process in all these cases, at the very least, an impartial judge, to whom camera tickets can be appealed, should be readily available. All tickets should be reviewed by a person.

Conflicting Data on the Safety Impact of Red-Light Cameras

Arguably, red-light cameras further the legitimate purpose of a limited government to protect citizens' rights to life and limb by deterring hazardous driving.

Several studies report that the use of such cameras deters the running of red lights and reduces accidents. In Scottsdale, Arizona, the use of red-light cameras reportedly brought about a 20 percent reduction in collisions in the areas where the cameras were deployed from 1997 to 1998. In Paradise Valley, Arizona, a 40 percent reduction in collisions is reported to have occurred between 1987 and 1998.[4] The use of red-light cameras in Mesa also reportedly reduced crashes at dangerous intersections between 7 and 16 percent.[5] According to the Federal Highway Administration, in Australia and the Netherlands the use of red-light cameras reduced incidents of running red lights by 35 to 60 percent.[6]

But not all studies show those same results. A 2000 study of red-light cameras deployed at intersections in Melbourne and Geelong, Australia, showed no fewer accidents or red-light running at intersections with cameras than at intersections without cameras. The authors said that lengthening the period of time during which both lights are red might be a simple, inexpensive countermeasure that could reduce accidents caused by red-light running.[7] Their results confirmed the findings of a 1995 study conducted in Victoria, Australia, which found that the presence of the cameras did not reduce the number of accidents at the sites, but actually increased the incidence of rear-enders.[8] A study by the Insurance Institute for Highway Safety promoted the benefits of red-light cameras based on data from Oxnard, California, but that study has been attacked because it did not actually study accidents caused by red-light running.[9] And the police chief of San Diego reported that the number of accidents went down at only two intersections equipped with red-light cameras, while increasing at four intersections, and remaining the same at nine intersections.[10]

Red-Light Cameras and Conflicts of Interest

A red-light camera can create a conflict of interest for whoever is operating it. The purpose of the camera is to deter red-light running. But if the system operators benefit financially from giving out tickets, the temptation is to ignore the system's main purpose, protecting lives, and turn it into a revenue raiser. Under these circumstances the system is unlikely to serve its legitimate purpose of reducing accidents.

This helps explain the mixed results of the San Diego system. As noted above, the number of accidents decreased at some intersections equipped with cameras and increased at others. The company with which the city had contracted to provide the camera service was paid per ticket. Documents revealed in a lawsuit to block the operations of the cameras revealed that the intersections chosen had been those that were most likely to yield violations, for instance, those with truncated yellow lights.[11]

This same conflict of interest is present in Arizona. In Mesa, Lockheed Martin, the camera contractor, is paid $48.50 for every $170.00 citation. In Paradise Valley, Redflex Traffic Systems is paid $35.00 per ticket. The integrity of the system would be vastly improved by paying the contractor a flat fee, or by paying the contractor for a reduction in the accident rate.

To conclude, there is no traditional principle of limited government that dictates that a camera can never be used as a substitute for the presence of a police officer. However, the potential for abuse is real, and there is a need for guidelines to limit the abuse of red-light cameras. Here are some suggestions:

- Red-light cameras should be used as a last resort. They should be used only when other measures, such as lengthening the duration of the yellow light[12] or the duration of the "all-red" period, fail to reduce the accident rate. In Mesa, Arizona, when three-second yellow lights were extended to four seconds, violations dropped 80 percent.[13] Changes in duration of yellow and red lights are far less expensive than setting up red-light cameras, several of which are operating at a financial loss in Arizona.[14]

- Yellow light intervals should be at least 4 seconds at intersections with approach speeds of 30 miles per hour or less and should be longer at intersections with higher approach speeds.[15]

- The parties responsible for operating the cameras should be rewarded for reductions in the accident rate or a reduction in red-light violations, never for the number of tickets handed out.

- No entity with a financial interest in awarding more tickets with the cameras should be involved with locating the cameras or timing the lights at camera-equipped intersections.

- The use of cameras at an intersection should be conspicuously posted on all approaching streets in advance of the intersection. This will increase the deterrent effect of the cameras and thus minimize the number of images that must be recorded.

- No tickets should be given in the case of an unclear camera image of either the license or the driver. No tickets should be given to anyone other than the actual driver of the vehicle. If the registered owner of the car is not the driver, a signed affidavit attesting to that fact should establish a presumption that the ticket is invalid, with the burden of proof on the state to prove otherwise.

- The use of images from red-light cameras by government employees for purposes unrelated to legal government functions should be forbidden and meaningful penalties for such abuses set forth.

- An impartial judge employed by an entity with no financial interest in awarding tickets should be available to process appeals of the tickets. All tickets should be reviewed by a person.

Privacy and Government in Arizona

Preserving Open Court Records Access

Since Norman times in England, common-law court proceedings have been open to the public.[16] There is a strong common law presumption that court records should be publicly available. The United States Supreme Court has recognized this, stating in *Craig v. Harney*[17] that "what transpires in the courtroom is public property." The Court continued, "there is no special perquisite of the judiciary which enables it, as distinguished from other institutions of democratic government, to suppress, edit, or censor events which transpire in proceedings before it." Elsewhere, the Supreme Court has affirmed that acquiring and disseminating information from court records is an important part of the right to free speech.[18] The principle that public records are open to the public is embodied in Arizona's open records statute; access to court records in particular is provided by Arizona Supreme Court rule 123.[19] Only in special circumstances may records be closed.[20]

Open records have long been recognized as an important aspect of officials' accountability in a free society. John Trenchard and Thomas Gordon, a pair of English authors, wrote a series of letters from 1720 to 1723, known as Cato's Letters, which helped lay the philosophical foundation for the American Revolution. In one of their letters, Trenchard and Gordon wrote, "it is in the Interest, and ought to be the Ambition, of all honest magistrates, to have their Deeds openly examined, and publickly scanned ."[21] Following in this classical liberal tradition, James Madison wrote that open records "safeguard against any attempt to employ our courts as instruments of persecution," promote the search for truth, and assure "confidence in . . . judicial remedies."[22] In criticizing the Sedition Act of 1798, Madison declared that the right to "freely examine public characters and measures, and of free communication thereon" was the "only effectual guardian of every other right."[23]

An Administrative Order issued by then Chief Justice Thomas Zlaket of the Arizona Supreme Court in August of 2000 created a committee to study the issue of public access to electronic court records. The order notes the increasing automation of court records access, and the "growing conflict between the public's interest in observing and knowing about its public institutions . . . and individual's [sic] interest in protecting private information from unwarranted intrusions through the use of sophisticated search engines." The committee's first draft report notes that the use of information in public records stored in paper format has neither the positive nor negative aspects of easy electronic access, because access to the paper records required a trip to the courthouse.

The committee has tentatively concluded that "traditional" access to records at the courthouse should be continued—the only conclusion consistent with free speech principles and the needs of the legal and financial community. More controversially, however, the committee is considering the following measures: (1) restricting remote electronic access to social security numbers and other sensitive information; (2) keeping

cases involving pre-sentence reports, domestic relations, juveniles, mental health, and probate off the Internet; and (3) restricting bulk access to case information. One of the most contentious issues has been whether access to social security numbers should be restricted in all cases, or only to the bulk of casual viewers accessing files over the Internet.

What follows are recommendations for resolving the continued need for open access to court records with concerns about highly sensitive information.

Bulk Data Access

The fact that bulk processing of the data in case files was cumbersome, if not impossible, in the days of paper files tends to make officials suspicious of the prospect of bulk data processing of this information made possible by new technology. However, there is no particular reason that records should not ultimately be made available in bulk electronic format for any lawful purpose, from legal investigations and fraud prevention to journalism and marketing. Having records available in bulk electronic format aids lawful businesses in supplementing informational databases used to prevent fraud and conduct employee background checks. The lack of availability of records in bulk electronic format almost always precludes their compilation for legal purposes by lawful businesses.

Internet Access

Court records should continue to be accessible for any lawful purpose. However, this need not be done by making the records openly available to the general public over the Internet. Opening records to the scrutiny of the idly curious may have unforeseen consequences, even if the display of the most sensitive information is blocked out. But records should be made available over other electronic networks to which access can be restricted, such as intranets within the courthouse.[24] And there is no good reason to deny remote access for lawful uses and users—including journalists, law firms, and financial firms—over secure electronic networks— perhaps virtual private networks. On a secure network, access to a record could be restricted if the subject of the record (perhaps a victim of domestic violence) has sought special protection, or if the user has been identified as a threat to the subject of the record. While this does not entirely satisfy all privacy concerns, the presumption in favor of open records is most consistent with the tradition of public trials and freedom of information.

Social Security Numbers and Sensitive Information

Social security numbers sometimes enable access to credit card accounts or other sensitive files. The publication of social security numbers in court records or other public files means that those accounts can also be accessed by perpetrators of credit-card fraud

or identity theft. Experienced investigators know, however, that at least half of all cases of identify fraud involve a perpetrator who knows the victim, such as a coworker, ex-spouse, or roommate.[25] Another significant number involve dumpster diving. But the risk of identify fraud overall remains low. Horror stories in the press tend to exaggerate the number of cases. The number of cases is usually estimated on the basis of the number of calls to telephone hotlines by victims who believe they might be victims of identity theft or credit fraud. But this number includes a significant proportion of false positives.

In the vast majority of cases, social security numbers help *prevent* fraud and the confusion of records. In a world where many people are named Tom Smith, it is important for every individual to have a more unique "name" that is never duplicated, and that remains constant across all his or her accounts. It is especially important given that 16 percent of the U.S. population moves every year, and there are about 2.4 million marriages and 1.2 million divorces every year, many resulting in name and address changes.[26] Attorneys, investigators, creditors, and financial companies rely on court records, including social security numbers, to track debtors and their liabilities, fugitives, witnesses, parents who owe child support, heirs, and missing persons. Blocking off such information from legitimate uses would throw sand in the gears of the legal and financial community.

Therefore, at most, social security numbers should be blocked out only in the version of records displayed over the Internet. Other "sensitive" information to be blocked out should be defined very narrowly. For example, information on loan amounts might be deemed too sensitive for display on the Internet. The risk of identity fraud and credit fraud is best addressed by aggressive prosecution and police investigation when it does occur. Also, consumers should be encouraged to take precautions, such as keeping sensitive documents out of site of coworkers and shredding statements and bills.

Freedom of Information and Privacy in the Private Sector

More Regulation for Consumer Privacy?

One bill (H.B. 2135) recently proposed in the Arizona legislature would require any Arizona-based entity that handles information about consumers to provide a privacy policy, access to the information, and an opportunity to opt out of transfers of the information to third parties. Many websites already offer an opt-out provision, but this bill would make an opt-out mandatory. The bill is worded generally and would affect those doing business on the Internet as well as other entities.

Although not as restrictive as a bill that requires companies to ask consumers to opt in before their information is shared, a broad opt-out rule would be a bad idea. Mandatory opt-out clauses are not consistent with some of the most beneficial types of information exchanges—those that help identify perpetrators of fraud, high-risk transactions, and errors. Credit reporting, for example, would not work if those who do not pay their bills could opt out of the system. Opt-out is also inconsistent with authentication systems used by electronic commerce merchants. These authentication systems comprise constantly updated lists of everyone's names and addresses. When a merchant gets an order, he checks it against the list to see if it matches a known name and address. If there is no match, the merchant knows to be alert to fraud or error. But if one can opt out of inclusion on the list, the merchant would have no idea if the lack of a match represents a problem or merely an opt-out. The usefulness of the database depends on its completeness.

The general premise behind the movement toward notice and opt-out requirements (as well as opt-in, discussed below) is that information exchanges between businesses are harmful to consumers. This is mistaken. Consumers may be unaware of the benefits, which economists are just beginning to measure, but the benefits are real nonetheless. Using information to target marketing can lower the cost to a business of each sale, from, for example, $9 to $2 per sale.[27] Those savings are passed on to consumers.

Information sharing allows for cost reductions. In the United States, cost savings from information sharing in financial services alone have been estimated at $17 billion per year for the customers of just one group of companies. (The savings would be larger still for the entire financial services industry.)[28] The availability of lists of consumer information also means more competition and consumer choice. This is because new businesses and new products rely on these lists to identify potential customers.

If a mandatory opt-out law is a bad idea, an opt-in rule would be a disaster. Opt-in is inconsistent with the basic principle that people should be free to exchange truthful information about real people and real events with one another. Because of low response rates to opt-in requests, opt-in effectively removes a significant amount of information about consumer preferences from the shared domain of facts and ideas. A study of the

apparel industry in the United States estimates that an opt-in rule would effectively impose a $1 billion tax on catalog and Internet clothing sales as businesses passed on an increase in costs of from 3.5 to 11 percent.[29] A recent study of an opt-in proposal in California concludes that adopting opt-in would cost California consumers, employees, and taxpayers billions of dollars, as well as shrinking the state's tax base by $2.1 billion.[30] For consumers who wish to avoid websites that do not offer an opt-out option, new P3P software and other programs are available.

Surfer Beware: The Web is a Public Area

Consumers new to the Internet may be operating under the illusion that their online activities are entirely private, unaware that their email may be tracked and read by local network administrators, that internet service providers record their data trails for billing and engineering purposes, that their screen names do not give them true anonymity, or that the websites they visit generally record their Internet Protocol addresses and may use cookies.[31] These consumers are mistaken. The essence of the Internet and other electronic networks is not privacy, but the seamless and low-cost transmission of information. Much of this information—temporarily assigned IP addresses, checksums used in error analysis, and so on—is of no particular importance other than the hardware and software that use it to network. Some of it is commercially valuable. A tiny amount of it is particularly sensitive or raises security concerns.

The bottom line is, no reasonably informed consumer should expect that his Internet traffic and messages are private, unless he or the site he deals with takes special measures to make it so. For this reason, the lack of a privacy policy is not deceptive. The default rule in human interactions is that when you interact with another person, he or she may learn something about you, and that is as true online as anywhere else. The next generation, raised with electronic networks, will be keenly familiar with the transparent nature of Internet communication.

The problem is that many of today's Internet consumers are not yet reasonably informed about the general lack of privacy on electronic networks. Should the law be adjusted to protect the uninformed consumer?

The Evolving Law of Internet Privacy Policies in Arizona

For cases involving Internet privacy policies, there already are laws on the books that prohibit deceptive trade practices, on or off the Internet. Perhaps taken with the novelty of the issue of Internet privacy, however, some prosecutors are going overboard. This section will review some actions of Arizona attorney general Janet Napolitano relating to privacy and offer guidelines for the future.

If consumers are not reasonably informed about Internet privacy, does that mean that attorneys general should charge websites with deceptive practices? In 2000,

Napolitano settled a case with a health care website that did not disclose its use of cookies in its privacy policy.[32] In most cases, prosecuting a company under these circumstances is misguided. Privacy policies need only describe uses of personally identifiable information, and cookies do not usually contain any information that can be traced back to a particular person, such as a name and address. Cookies can only be associated with such information as a name and address if users provide this information voluntarily and the site deliberately links the two.[33] Because most consumers do not understand Internet technology, the attorney general's office seems to have concluded that consumers are entitled to assume that information collection and sharing is not going on.

Good-Faith Changes in Privacy Policies

A company may post a privacy policy in good faith but wish to change it, or may unwittingly violate it in some trivial manner. A good example is Toys R' Us, which promised not to share information with third parties. However, the company continued its usual practice of sharing purchasing data with a consultant who processed the information to advise the company about product placement and other customer service issues. It had not occurred to the drafters of the privacy policy that their usual business partner would be considered a "third party," and the company found itself facing threats of action by several state attorneys general, including Arizona attorney general Janet Napolitano. But although the company made a mistake, there was no harm to consumers as a result of that mistake. Toys R' Us ultimately settled with the various states and clarified its privacy policy, though it admitted no wrongdoing. In the future, Arizona's attorney general should devote scarce prosecutorial resources to cases involving credit card fraud, identity theft, and other real crimes.

The rule should be that only a consumer's *reasonable* expectations of privacy are implied into the contract between the parties. To allow a lawsuits to go forward when a consumer's expectation of privacy is based on ignorance is to, in effect, reward naïveté—to give the careless consumer more protection than the alert consumer. Businesses should not be liable for consumers' wrongful expectations. A business can reasonably be expected to anticipate what an *informed* consumer will do. But a business cannot reasonably be expected to anticipate what consumers may wrongly believe, because the universe of wrong beliefs is infinite.

Furthermore, most of the information transferred back and forth over networks regarding consumers' Internet behavior can be shared among legitimate businesses with absolutely no harm to consumers. Consumers benefit when businesses learn more about their preferences.

As with any other contract terms, businesses and consumers alike benefit from some flexibility. Overzealous prosecution will simply "chill" electronic business. One effect will be to discourage privacy policies that promise real protection. Fearful of being "locked in" to money-losing privacy policies by prosecutors, businesses will be reluctant to experiment by offering consumers extra protection for their privacy.

Suggested Guidelines on Deceptive Privacy Policies

Listed below are some guidelines for determining when privacy policies or the lack thereof should be considered "deceptive."

? The mere lack of information about a company's information-sharing practices is not deceptive, nor should information sharing be presumed harmful.

? Businesses should not be accused of deception because consumers choose not to acquaint themselves with basic Internet technology. Consumers choose how much to research privacy issues like cookies or encryption. Some consumers may choose not to allocate any time to researching these issues and may instead spend their time researching the price or quality of merchandise. These are legitimate consumer decisions, as most business uses of information are beneficial or neutral with regard to consumers' well-being.

? When a company has violated the terms of its privacy policy, it may have committed a deceptive practice, but prosecution should be low priority in cases in which no actual harm was done to consumers.

? The most rewarding targets for prosecutors in terms of real benefits to consumers are not hapless websites, but perpetrators of credit card fraud, identity theft, or other real crimes. Scarce prosecutorial resources should be focused on those crimes.

? Companies should not be "locked in" to their privacy policies forever; good faith changes in contract terms are an ordinary part of commercial life.

Conclusion

Both freedom of information and privacy are important constitutional and common law traditions in the United States. Freedom of information is and should be the general rule, with confidentiality being protected where there is solid proof that it is necessary to prevent a real harm. The movement of information throughout the economy generally benefits consumers by preventing fraud and lowering the prices of products. Moreover, information is important to the legitimate functions of government. The market will and does respond to consumer demands for privacy.

Prosecutors and lawmakers should focus tightly on real harms to consumers such as credit fraud or identity fraud rather than pass broad laws that tangle legitimate businesses and consumers in the legalese of notice and choice provisions. However, in the case of government intrusions into private space, broader, more general protections from privacy at the constitutional level are necessary. At the same time, it is not necessary to cut government off from the use of new technologies entirely, if those responsible are held accountable for abuses.

Notes

[1] Joey Ledford, "Smile! You're on Red-Light Camera," *The Atlanta Journal-Constitution*, July 30, 2001, www.accessatlanta.com/ajc/horizon/horizon0730/cameras0730.html. "Arizona has a far higher rate of fatal red light running crashes than other states." Insurance Institute for Highway Safety, "Red Light Running Factors into More Than 800 Deaths Annually," News Release, July 13, 2000, www.hwysafety.org/news_releases/2000/pr071300.htm.

[2] "Red light cameras are judge, jury and executioner all in one box." Dick Armey, "The Red Light Camera Danger," *Freedom Works*, July 17, 2001, http://freedom.house.gov/auto/news/danger.asp

[3] Partly because of intense heat, red-light cameras in Tempe and Mesa fail to produce clear enough images in two out of three cases. In about one in every five cases, the view of the driver's face is blocked.

[4] American Traffic Systems, "Safety Results," www.atstraffic.com/safety/default.htm.

[5] Janet C. Vinzant, "Evaluation of the Effects of Photo Radar Speed and Red Light Camera Technologies on Motor Vehicle Crash Rates," March 1, 1999, www.ci.mesa.az.us/police/traffic/march_1999_report.htm.

[6] Federal Highway Administration, "FHWA Study Tour for Speed Management and Enforcment Technology," December 1995, p.9, http://ntl.bts.gov/DOCS/speed06.html.

[7] S. Kent, B. Corben, B. Fildes, and D. Dyte, "Red Light Running Behavior at Red Light Camera and Control Intersections," Monash University Accident Research Center Report no. 73 (2000), p. 2, www.general.monash.edu.au/muarc/rptsum/es73.htm.

[8] David Andreassen, "A Long Term Study of Red Light Camera and Control Intersections," Australian Road Research Board, February 1995, p. 22, http://freedom.house.gov/auto/rlcdocs/95aussie.pdf.

[9] Andrew LeFevre, "Red Flagging Red-Light Cameras," 3 American Legislative Exchange Council Policy Forum (Winter 2001/2002), 36-37.

[10] "Case Closed: No Safety Benefit to Red Light Cameras," *Freedom Works*, July 30, 2001 (quoting San Diego police chief David Bejarano as seen on ABC's *Nightline*), available at http://freedom.house.gov/library/multi/bejarano.asp.

[11] For an article referring to the case, see "Big Brother's Camera," Editorial, *Wall Street Journal*, July 3, 2001, p. A14.

[12] Increasing the time of yellow lights from 4.0 to 5.5 seconds decreased the number of red light violations at two intersections in Fairfax, Virginia, by 96 percent. National Motorists Association, "Red Light Citations Drop Below One per Day," Press Release, July 12, 2001, www.motorists.org/issues/enforce/vastudy.html .

[13] Ledford, p. 4.

[14] Ibid. The Mesa program had lost $14,621 by mid-2001, and the Phoenix program was budgeted for a $250,000 shortfall the same year.

[15] National Motorists Association, "Model Red Light Camera Law," www.motorists.com/issues/enforce/rlcmodellaw.html.

[16] *Richmond Newspapers, Inc. v. Virginia*, 100 S. Ct. 2814, 2821-2817 (1980) (describing the history and tradition of the open trial in England and America).

[17] *Craig v. Harney*, 331 U.S. 367 (1947).

[18] Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 95 S.Ct. 1029, 43 L.Ed.2d 328 (1975).

[19] Arizona Revised Statutes Annotated § 39-121.

[20] See, for example, *Arizona Board of Regents v. Phoenix Newspapers, Inc.*, 806 P.2d 348, 351 (Ariz. 1991), describing the principle protecting privacy when disclosure could cause "substantial and irreparable private or public harm" (internal citation omitted).

[21] Timothy B. Dyk, "Newsgathering, Press Access, and the First Amendment," *Stanford Law Review* 44 (1992): 959, quoting Trenchard and Gordon in Leonard W. Levy, *Emergence of a Free Press* (New York: Oxford University Press, 1985), p. 110.

[22] James Madison, Letter to W. T. Barry, August 4, 1822, in *The Writings of James Madison* 9 (Hunt ed. 1910), p. 103

[23] James Madison, "Report of the Committee to Whom Were Referred the Communications of Various States, Relative to the Resolutions of the Last General Assembly of This State, Concerning the Alien and Sedition Laws (Virginia House of Delegates, 1799-1800)," in *The Mind of the Founder: Sources of the Political Thought of James Madison*, ed. Marvin Meyers (New York: The Bobbs-Merrill Company, 1973) p. 315.

[24] Those who are motivated by idle malice will be less likely to take the time to travel to courthouses and negotiate the security obstacles blocking access to intranets.
[25] www.cspra.org/csprasite/pdfs/identitytheft.pdf.
[26]The Coalition for Sensible Public Records Access, "Identity Theft," www.cspra.org/csprasite/pdfs/identitytheft.pdf.
[27] See J. Jovan Philyaw, CEO of DigitalConvergence.com, in a transcript of "A Cato Institute Roundtable: Privacy vs. Innovation," May 7, 1999, p. 48 (describing use of information to lower costs from $9 per order to $2).
[28] Ernst & Young for the "Financial Services Roundtable, Customer Benefits from Current Information-Sharing by Financial Services Companies," December, 2000, www.bankersround.org/PDFs/custbenefits.PDF.
[29] Michael A. Turner, "The Impact of Data Restrictions on Consumer Distance Shopping," 2001, www.understandingprivacy.org.
[30] Peter A. Johnson, "The Hidden Costs of Privacy: The Potential Economic Impact of 'Opt-In' Data Privacy Laws in California," Progress and Freedom Foundation, January, 2002.
[31] The Internet Protocol (IP) address is the Internet equivalent of a telephone number—it allows machines in one part of a network to locate those in another part. Unlike a telephone number, however, your IP address may change every time you log on to a network, because your internet service provider may assign you the number only as long as your are on its network. A "cookie" is a tiny bit of information that is stored temporarily or permanently on your hard drive. Cookies tell the website whether someone using your computer has visited their site before. Cookies allow us to "pile up" goods in an electronic shopping cart, and enable other basic electronic commerce functions. They are also used to measure the number of times a user has seen a particular banner ad.
[32] Arizona attorney general Janet Napolitano, Press Release, Dec. 18, 2000, www.attorney_general.state.az.us/ press_releases/dec/121800.html. This reports the attorney general's having settled with HealthSquare.com for failing to mention the use of cookies in its privacy policy promising confidentiality; the company was required to clearly state in its privacy policy if it uses cookies, how it uses cookies, and what cookies are, as well as pay $1,500 in attorney's fee and costs.
[33] Glenn Fleishman, "Cookies: Fresh From Your Browser's Oven," December 17, 2001, www.webdeveloper.com/cgi-perl/cgi_fresh_cookies.html.