

THE TENSION BETWEEN PRIVACY AND SECURITY: AN ANALYSIS BASED ON COASE AND PIGOU

KATHLEEN WALLMAN*

| | |
|---|-----|
| INTRODUCTION..... | 397 |
| I. WHY IS THERE A TENSION BETWEEN PRIVACY AND SECURITY? | 398 |
| II. WHAT IS PRIVATE? | 399 |
| III. WHAT IS SECURE?..... | 401 |
| IV. PIGOU AND COASE | 402 |
| V. APPLYING PIGOU AND COASE TO THE TENSION BETWEEN PRIVACY AND SECURITY | 404 |
| VI. THE DYSTOPIAN FUTURE | 406 |
| CONCLUSION | 407 |

INTRODUCTION

The tensions between privacy and security are ample. Legions of writings document the intrusions that readily available technologies wreak upon privacy. Justice Scalia, in his pathbreaking opinion in *Kyllo v. United States*,¹ foresees a world in which Radio Shack supplies invasive devices for the merely curious as well as the pruriently motivated to check on neighbors, friends, and enemies.

The ways in which security demands challenge privacy rights are well documented, and, to some extent, obvious at the intuitive level. But what is more interesting is whether the United States legal system, and

* Visiting Research Professor, Georgetown University, former Deputy Assistant to the President for Economic Policy and Counsellor and Chief of Staff to the National Economic Council, Deputy Counsel to the President, Chief, Common Carrier Bureau, Deputy Chief, Cable Services Bureau, Partner, Arnold & Porter, Law Clerk to the Honorable Laurence Silberman and the Honorable Edward Tamm, U.S. Circuit Court for the District of Columbia, and the Honorable Pauline Newman, U.S. Circuit Court for the Federal Circuit. J.D., Georgetown University Law Center, M.S.F.S. Edmund A. Walsh School of Foreign Service, Georgetown University, B.A. Catholic University of America. Thanks to Steve Wallman and Elizabeth Lyle for reading drafts of this article, and to Phil Weiser for all of his help.

1. 533 U.S. 27 (2001).

the society it serves, can find and define an appropriate spot on the spectrum that maximizes the majority's privacy rights and personal security.

I suggest in this essay that the United States has found a Pareto-optimizing² solution to the tension between privacy and security by externalizing it to non-native American citizens and resident aliens. Worse yet, from a civil libertarian perspective, this burden of externalization falls disproportionately on parties not judged guilty or liable under the criminal laws, but are convenient "recipients" of this externalization because of their countries of origin or religion.

I. WHY IS THERE A TENSION BETWEEN PRIVACY AND SECURITY?

Jeremy Bentham postulated a horrific but effective way of controlling the behavior of incarcerated individuals: the Panopticon.³ The concept of the Panopticon was a structure in which the incarcerated person was sheltered in a structure that allowed the prison guards to watch the incarcerated person at all times, but to do so unseen by the incarcerated person.⁴ The lighting in the hypothetical structure was such that the incarcerated person was visible, always, in silhouette, to the prison guards, whose gaze upon the incarcerated person was disguised by the lighting scheme.⁵ Of course, the prison guards were not at all times looking at a particular incarcerated person – but, from the perspective of the incarcerated person, the guards might be training their gaze upon him or her. Hence, the apparently constant supervisory effect was the same regardless of whether it was in fact constant, and the disciplinary effect on the incarcerated person was achieved.

The guards in Bentham's Panopticon had it easy, in a sense. They knew whom to supervise, and the number of prisoners was limited in the sense that it was less than the entire population of the country. But imagine translating this experiment to the entire United States. How? Successful translation of this experiment would require that everyone in the United States feel or believe that he or she was being watched, or might be under surveillance, at all times. Under what circumstances would this be acceptable? If the increase in perceived or actual security outweighed the cost imposed by this real or perceived intrusion on

2. A Pareto optimized or Pareto efficient outcome is one in which resource allocation choices have maximized the welfare of all actors, and none can become better off without at least one other actor becoming worse off. See PAUL A. SAMUELSON, *ECONOMICS* 460 n.12 (9th ed. 1973).

3. JEREMY BENTHAM, *THE PANOPTICON WRITINGS* (Miran Bozovic ed., Version 1995) (1787).

4. *Id.*

5. *Id.*

privacy, this bargain might be acceptable. Alternatively, it might be acceptable if Americans believed that the tax on privacy imposed by increased security, while evenly levied across the population, was being disproportionately collected from people who “deserved” this additional tax. That is, while everyone pays the tax by accepting surveillance, most people regard their own payment as trivial in terms of the practical restrictions upon their activities and freedom. But they believe that others will regard the restrictions as substantial, not trivial. Thus, the tax payment collected from these other people is disproportionately dear to them. In the context of this analogy, law enforcement and national security authorities function as the tax collectors.

II. WHAT IS PRIVATE?

This question is relevant because it helps establish how difficult or easy it is to impose a tax on privacy. If the boundaries of the privacy right are fluid and shrinking because of technological advances and uncertainties about how the courts will treat them, as argued here, then the tax is easier to collect. If the tax is easy to collect, that is, the tax collectors’ transaction costs are low, the tax collectors can behave more decisively or even aggressively in their collection efforts. This may have implications for choices about the preferred mechanism for striking the balance between privacy and security: a government imposed tax, as might be advocated by Pigou, or a private bargaining solution, as might be advocated by Coase.

The suite of privacy protections at work in the United States is composed of both practical and legal protections. The legal sources are well known and well tested, although technology pushes the boundaries of this protection in notable ways in the jurisprudence. Although the word “privacy” appears nowhere in the Constitution, several amendments to the Constitution are commonly understood and interpreted to protect privacy. The Third Amendment protects privacy in the sense of prohibiting the bivouacking of troops in private homes except in wartime.⁶ The Fourth Amendment protects the right of the people to be secure in their homes and effects from unreasonable searches and seizures.⁷ The Fifth Amendment protects people against self-incrimination, which is a way of protecting the privacy of certain utterances.⁸ The Fourteenth Amendment imports the protection of these federal protections to the citizens of the states,⁹ and, most

6. U.S. CONST. amend. III.

7. U.S. CONST. amend. IV.

8. U.S. CONST. amend. V.

9. U.S. CONST. amend. XIV.

famously, in its penumbra, protects the species of the right of privacy that allows procreative freedoms.¹⁰

The practical protections of privacy are less well defined and shift with available technology. The most honored and hermetically sealed way of protecting privacy is not to tell anyone, and to make no record of the information for which privacy is sought. At least until means are invented to discover the thoughts in an individual's head, this method is reasonably likely to maintain privacy.

But once the information is outside the individual's own head, the gamble begins. Telling someone else a "private" fact compromises its privacy as a practical matter since that confidant may breach trust and tell others. But the extent to which privacy is compromised as a legal matter may depend crucially upon the role of the confidant. Privileges such as the physician-patient privilege and the attorney-client privilege shield disclosures in these contexts from official discovery through legal compulsion. The privilege of the confessional shields the penitent's admissions from discovery. But these privileges are heavily qualified by exceptions and, as developed below, are even more heavily qualified in the post-September 11 environment.

A written record of a private fact raises the stakes even higher. Some such written records are made at the option of the individual for whom the fact at issue is private, such as the now famous diary of former Senator Bob Packwood, or the equally famous diary of Joshua Steiner, Treasury aide during the Clinton Administration.¹¹ Such private writings, in both cases, became the subject of official inquiry when the "right question" popped up during the course of interviews or depositions.

Technological developments further challenge privacy. Surveillance cameras, once so novel in the United States that a special deployment of them at a Superbowl game caused controversy, are now commonplace in urban areas.¹² They have long been a fact of life in other countries such as Great Britain. Satellite photographic surveillance, once the exclusive purview of sovereign entities that could afford to launch and maintain the equipment, is now in the public domain.¹³

10. See, e.g., *Roe v. Wade*, 410 U.S. 113 (1973); *Planned Parenthood v. Casey*, 505 U.S. 833 (1992).

11. Linton Weeks, *Scandal May Mean the End of White House Diaries*, THE WASHINGTON POST, March 4, 1998, at D01.

12. JOHN D. WOODWARD, SUPER BOWL SURVEILLANCE: FACING UP TO BIOMETRICS (Rand Arroyo Center, IP-209, 2001), available at <http://www.rand.org/publications/IP/IP209/IP209.pdf>.

13. For example, visit TerraServer's website to insert your home address and see historical satellite photographs of your house and neighborhood. TERRA SERVER, at <http://www.terra-server.com> (last visited March 13, 2005).

Biometrics, including fingerprints, face recognition, and retinal scans, suggest ways that uniquely identifying information about individuals could be captured and used later to identify the individuals.¹⁴ Problems abound, however, in deploying this system. First, how should the compilers of the database collect the information when not everyone of interest will be a willing contributor of information? Second, once the information is collected, say, at ports of entry or in consular offices abroad, to which database should the information be compared? There currently exist databases such as the National Crime Information Center's database, but there is no comprehensive public safety and national security database reference against which collected biometric information can be compared.

Nanotechnology is a futuristic challenge to privacy that is fast racing toward the present. Current deployments of nanotechnology involve implantation of microscopic radio frequency identification tags that can be read from short distances by receivers.¹⁵ They are useful in inventory management, for example. But the future uses are suggestive of truly troubling challenges to privacy. Radio Frequency Identification (RFID) tags implanted in clothing, wallet cards or under the skin might verify an individual's presence at an airport, or a library, or a church. Its one current, significant limitation is that the power level of the chip is quite low so as not to interfere with other RF devices. If this limitation is eventually overcome so that RFID tags have long-range locational capabilities, "where are you?" may become a question that no one ever has to ask again.

These tools are cause for discomfort for everyone subject to the modern Panopticon because it diminishes the possibility of hiding from the Panopticon or preserving a perception, however illusory, of personal privacy. But the cost of this sacrifice is hard to quantify, while the touted benefits of increased security seem hard for many people to overvalue.

III. WHAT IS SECURE?

It is difficult to place a value on security for purposes of evaluating the balance between privacy and security because security is a relative concept. Even the most confident advocate of public safety and national

14. In 2004, the United States modified its immigration arrival protocols to require visitors to provide fingerprints upon arrival in the U.S. as a prelude to requiring more comprehensive biometric identification. The program received criticism from countries such as Brazil whose citizens were subject to the fingerprinting requirement. See *U.S. Starts Fingerprint Program* (Jan. 5, 2004), <http://www.cnn.com/2004/US/01/05/fingerprint.program/>.

15. See Vanessa Carey Pert, *Sleepwalking in a Wireless World: How Will Wi-Fi and RFID Evolve?* (Apr. 27, 2004) (Masters Thesis, available at <http://cct.georgetown.edu/thesis/VanessaPert.pdf>).

security would have to concede that absolute security – an environment completely free of risk of security threats – is impossible to create in a way that is compatible with the normal business of life.

Security is essentially a measure of risk.¹⁶ This is partly based on historical statistical information. For example, the risk of having a car crash on Labor Day weekend can be understood based on historical information. The risk of a plane crashing can be understood based on how often such an event happens per thousands of flights. Another important dimension of risk measurement is the fallout of an event occurring, even an unlikely event. The risk of an intercontinental nuclear warhead exploding in a populated part of the world is probably small, but worth applying cautionary measures to prevent because the consequences would be catastrophic.

But translating statistical risk to the individual is a more emotional and less rational process. Many people have greater fear of dying in a plane crash than in a car crash, although they are much more likely to be involved in the latter than the former. Likewise, many people fear their own involvement or a loved one's involvement in a terrorist incident than they do involvement in a car crash. The reasons for this are various, but seem mostly to have to do with the relative lack of control over things like plane flight and terrorist ambitions, in contrast to familiar everyday things like driving a car. This lack of control creates a sense of anxiety, which in turn diminishes the sense of security.¹⁷

Thus, the process of increasing security involves two parts. The first is to control and reduce the statistical incidence of the harmful act. The second is to decrease the sense of anxiety about those aspects of the harmful acts that might occur in the future. The contributions of Pigou and Coase suggest conceptual frameworks for the ways in which the United States has pursued this agenda.

IV. PIGOU AND COASE

In the dialectic of economic thought and literature, there is likely no more famous duo than Arthur Pigou and Ronald Coase. Pigou's work, *The Economics of Welfare*,¹⁸ developed the concepts of public goods and externalities and made the case that government had a necessary role in

16. ROSEN, THE NAKED CROWD (2004). See Ch. 2, *The Psychology of Fear*.

17. For many years, the Roman Catholic Mass has included a petition, following the Lord's Prayer, that God "deliver us . . . from every evil, . . . and protect us from all anxiety. . . ." DAUGHTERS OF ST. PAUL, VATICAN II SUNDAY MISSAL MILLENNIUM EDITION 642 (2002). The connection between a felt lack of control and anxiety is not a modern neurosis.

18. ARTHUR C. PIGOU, THE ECONOMICS OF WELFARE. (Transactions Publishers 2002) (1920).

controlling the generation of negative externalities through taxes and subsidies. The theory is illustrated by environmental regulations that seek to discourage pollution by taxing the activity that produces the pollutants, along the lines of the carbon tax proposed in the Kyoto Treaty on Global Warming.

Pigou's work came under attack from various quarters, but none as decisively true in aim as from the work of Ronald Coase.¹⁹ Coase argued and proved that there were private bargaining solutions to the problem of externalities, and that government intervention by means of taxes and subsidies was not always necessary.²⁰ The example of the polluting neighbor illustrates the point.²¹

Assume that a chemical factory is located next to a farm. Periodic accidents that occur in the course of normal production at the chemical factory spew harmful chemicals on the crops next door. This results in the ruin of the crops and causes financial injury to the farm and its owners. Assume that the two businesses are located in a state with minimal governmental prohibitions against chemical pollution, or at least minimal resources or inclination to enforce them – say, New Jersey. The Pigou solution to this problem would be to have the government tax the chemical factory to the point where production would decrease, and accidents in the normal course of production would decrease commensurately. Additionally, or alternatively, the operators of the chemical factory might take greater care to avoid accidents, and increase internal expenditures to that end.

Coase's solution to this problem would be to have the parties engage in private bargaining. The chemical factory operators would determine how much each additional unit of production is worth to them. The farmer would determine how much each ruined unit of crop production costs. In the zone of overlap between those two figures, a mutually beneficial deal was possible. So if each additional unit of chemical production is worth three dollars, and each bushel of ruined potatoes is worth four dollars, the farmer should be willing to pay the chemical factory operators up to four dollars to cut back production, and the chemical factory operators ought to be willing to accept something between three and four dollars to forgo producing additional units of its product. There are many caveats to the operation of this elegant and possibly utopian solution. Transaction costs must be zero, in other words, the three dollar and four dollar figures must encompass all the costs on both sides, which rarely pertains. The parties must have access

19. COASE, *THE FIRM, THE MARKET, AND THE LAW* (1988). See particularly Chapter Five.

20. *Id.* at 95-96.

21. *Id.* at 97-04.

to one another, apply rational bargaining skills, and have relatively equal bargaining power, at least as to the matter at hand. To witness perfect application, the government must not put its thumb on the scale in favor of either party to the possible private bargain. But it plausibly suggests that there is another way altogether for dealing with conflicts and tensions between parties: engineering government taxation as Pigou suggests, letting the affected parties strike a bargain as Coase suggests, or introducing the government as an intermediary in and enforcer of a tacit private bargain between the affected parties.

V. APPLYING PIGOU AND COASE TO THE TENSION BETWEEN PRIVACY AND SECURITY

The theories of both Pigou and Coase address the issue of controlling externalities – promoting positive ones and discouraging behavior that expands negative externalities. To the extent that the tension between privacy and security generates externalities, the approaches of Pigou and Coase may be useful in balancing that tension, or at least understanding it.

A negative externality is a spillover cost that can be pushed off to parties other than the ones generating the cost.²² I believe that the fundamental reason that there is a tension between privacy and security is that the perceived need for security generates an externality: the perceived need for greater surveillance, and sacrifice of privacy, on someone's part, in order to increase security or perceived security. In order for people to feel more secure, people must be watched more closely in order to inhibit the likelihood of action by some people that might impinge upon security. The increase in security might be real or only perceived, but in order for either to be achieved, surveillance must increase.

But increased scrutiny and surveillance are at odds with the basic freedoms and civil liberties that are embedded in U.S. society. How will citizens become convinced that this trade off is worthwhile? I suggest that an important element of this case of self-persuasion is for a majority of the people to become convinced that the increased scrutiny will occur at no price to their personal privacy; rather, the imposition will be felt by others to whom the intrusion is justly applied.

The role of the government as tax collector is important here. While Panopticon style surveillance may be applied to all, the government can collect a heavier tax on privacy through additional

22. See Martyne M. Hallgren & Alan K. McAdams, *The Economic Efficiency of Internet Public Goods*, in INTERNET ECONOMICS 458-59 (Lee W. McNight & Joseph P. Bailey eds., 1997).

surveillance applied to some who are deserving of this additional scrutiny. It is the government's unique ability to redistribute the cost of the sacrificed privacy that makes the surveillance and attendant sacrifices generally acceptable. In this way, the government is playing a role that is to some extent, on the one hand, in line with that described by Pigou – imposing a tax to discourage a negative behavior – and, on the other hand, that conceived by Coase as an intermediary in a bargain between two groups of private actors. One group of private actors, the persons upon whom the disproportionate burden of collection falls, well may be an unwilling party to the bargain, but a party nonetheless because of the government's power to require compliance.

This is where intelligence gathering comes into play, identifying, for example, individuals (a) who have traveled to certain areas, *e.g.*, Afghanistan, (b) who have engaged in certain forms of speech, or (c) who have associated with certain types of organizations or individuals. Often the sources of intelligence are mysterious to the public, but in the current environment, doing something about a perceived threat has lately yielded situations in which the authorities have had to convey something about what concerned them. Take, for example, the numerous flights between Europe and the United States and Mexico City and the United States that were cancelled around the 2003 year-end holidays.

But the intelligence screens appear to produce results that have one theme in common: they focus on foreign nationals in the United States, or naturalized United States citizens. In both cases, the focus is cast mostly on persons from nations classified as suspect or associated with heightened risk.

The reality that this approach produces is to identify a relatively disenfranchised segment of the population to which heightened security scrutiny is applied. The cost of acquiring increased security, real or perceived, is externalized to this segment of the population.

And a majority of Americans seem relatively comfortable with this externalization. A Gallup Poll survey taken immediately after September 11, 2001, found that 58 percent of those surveyed would favor Arabs, including U.S. citizens, undergoing special, more intensive security checks at airports before boarding planes.²³

At the same time, a more recent poll shows that Americans regard basic freedoms such as the right to privacy and the right to due process as crucial or very important – two of the very types of rights at stake in the

23. DAREN K. CARLSON, THE GALLUP ORGANIZATION, DOES FREEDOM RING IN THE AGE OF HOMELAND SECURITY? (2004), *available at* <http://www.gallup.com/poll/content/login.aspx?ci=10300> (subscription required).

increased scrutiny to which some people will have to be subject in order to make others feel secure.²⁴

This analogy has limitations. Both Coase's and Pigou's analyses depend upon the existence of clear, quantifiable rights. But the right to privacy is evolving in light of law and technology, and its boundaries are fluid and shrinking in that same light. It is of different value to different individuals. The externality at issue here, unlike the ones in Coase's and Pigou's examples, are not generated in commercial transactions, which further compounds the issue of quantification. But the framework offered by both bodies of theory regarding how to deal with a cost generated by one party that falls upon another is nevertheless instructive.

VI. THE DYSTOPIAN FUTURE

One way of understanding this cognitive dissonance²⁵ between how much Americans value their freedom and how they are willing, at the same time, to trade others' privacy to enjoy their freedoms with more security is through the insights provided by Pigou and Coase on externalities. Although Pigou and Coase disagreed on feasible and optimal ways of handling externalities, they agreed that when transactions produced them, they could be allowed to burden those upon whom they naturally fell or reallocated. Pigou envisioned doing this by government intervention; Coase by private bargaining, at least in certain circumstances.

It is possible that the externalities created by intrusive approaches to security are subject to a combination of the approaches of Pigou and Coase. The taxation analogy that invokes Pigou's approach is inexact for the reasons acknowledged above, yet the government plays a definite and important role in determining how the burden of privacy-invasive responses to security issues will fall. Perhaps the government is partly playing the role of tax collector as envisioned in the analogy presented above, but, equally important, is also playing a role as an intermediary in a tacit and otherwise difficult to organize private bargain between a majority willing to accept tradeoffs to their privacy and a minority that is ill-positioned to complain.

24. Eighty-nine percent of those surveyed said that the right to due process was crucial or very important to them; 91 percent said that the right to privacy was crucial or very important to them. *Id.*

25. Cognitive dissonance is defined as a "[m]otivational state produced by inconsistencies between simultaneously held cognitions or between a cognition and behavior, *e.g.*, smoking, enjoyment and believing smoking is harmful are dissonant." MEDICAL DICTIONARY, COGNITIVE DISSONANCE, at <http://www.books.md/C/dic/cognitivedissonance.php> (last visited Mar. 13, 2005).

In this way, externalizing the cost of this seemingly enhanced privacy to a minority that is less well positioned either to ask the government to spread the costs more evenly – Pigou’s solution – or to bargain its way back to parity – Coase’s solution – makes it possible for Americans to place a high value on their own privacy, while accepting intrusive approaches to security problems precisely because they believe that the cost will not be theirs to bear.

CONCLUSION

It is fair to ask what this means and whether it is a problem worth addressing. At the very least, the externalizing of privacy costs to minorities is problematic, if not domestically, then certainly in terms of the United States’ advocacy abroad of democratic institutions and processes. If the intended beneficiaries of democratic reforms come to understand that the occupiers of Iraq, for example, or their designated successors, will fail to enforce norms that protect minority rights and access to privileges, then the job of reform will be all the more difficult and dangerous. Privacy rights are just one example of the type of norm that the intended beneficiaries of reform might look to as a way of understanding what might be in store.

