FINANCIAL PRIVACY AND THE THEORY OF HIGH-TECH GOVERNMENT SURVEILLANCE

PETER P. SWIRE*

How would you like the government to have access to the records of every purchase you have ever made? Most people feel some sort of chill at that prospect. Although it may be difficult to pinpoint the problem, many people would feel a loss of freedom and would have a range of other worries about living in a society where every purchase left inerasable tracks. This Article examines the topic of financial privacy. One goal of this Article is to help develop the vocabulary of what might be wrong with too ready government access to transaction records. An overlapping concern, discussed more fully in other writings, is how to assess the desirability of private-sector access to personal financial information.[1]

There is a privacy paradox, however. In the long term and taking a broad view, most people are concerned about invasions of privacy that might result from government access to sensitive financial and other records. But in the short term, when particular uses of data are at stake, the political system and many people prefer to let the information be used rather than to uphold privacy values. Examples include requiring deadbeat parents to pay child support or tracking the profits of drug smugglers and other money launderers. In such instances, access to financial data is seen as an important tool for effective law enforcement. The paradox is that people seem to have a long-term concern for privacy while making short-term decisions not to respect it.

Now is an important time to put those short-term decisions into longer-

---

* Chief Counselor for Privacy, United States Office of Management and Budget; Professor (on leave) Ohio State University College of Law. The text of this paper was completed before the author entered the United States Government, and the views expressed herein are entirely his own. For helpful comments, the author thanks Ruth Colker, Jody Kraus, Mark Lemley, Alan Michaels, Alan Westin, and participants at On-Line Offshore '98, the Telecommunications Policy Research Conference '98, an Ohio State Law Faculty Workshop, and the Brookings Wharton 1998 Conference on Financial Services. Research assistance was provided by James Collum, Mark Davis, and Jane Higgins. Financial Support for this project came from an Ameritech Faculty Fellowship, the Brookings Institution, and the Ohio State University College of Law. An earlier version of this paper was published in the Brookings Wharton Papers on Financial Services 1999.

1. *See* PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 90-101 (1998); Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE 3 (1997); Peter P. Swire, *The Uses and Limits of Financial Cryptography: A Law Professor's Perspective* (visited Feb. 18, 1999) <http://www.osu.edu/units/law/swire.htm> [hereinafter Swire, *Financial Cryptography*].

term perspective. As discussed in Part I, payment systems are shifting to more electronic and more traceable payment mechanisms. The traditional cash transaction left no automatic link between the transaction and the purchaser's name. The modern debit or credit card, by contrast, automatically places the purchaser's name into a data file, at least potentially available to public and private entities after the fact. To get a preliminary sense of the harms that can arise from traceability, Part I invites the reader to consider the problems of identity theft, the problems of having government access to each book and web page that an individual has accessed, and the risks of having an authoritarian or totalitarian government being able to trace every financial transaction within its borders. With these harms in mind, this Article proposes an anatomy of harms that can arise from financial or other government surveillance: the harms themselves; chilling effects, or activities foregone due to surveillance; cloaking costs, or actions taken to evade surveillance; and the burdens of having to comply with surveillance requests.

Part II introduces the metaphor of data entering a "vault 600 feet down," and uses that metaphor to understand the range of ways that data can "reach the surface," or become accessible. Good procedures, such as careful judicial oversight, can limit problems that might arise from personal financial data flowing out of the vault. Where such procedures are not effective, however, society may decide to allow data to be filtered before it enters the database. In other words, anonymous financial transactions may be desirable in certain circumstances, even in a future Internet payment system, just as anonymous cash payments are common today.

Part III systematically examines the advantages of government access to financial transaction data. The government has a strong interest in receiving data relevant to its own financial affairs, such as collection of taxes and distribution of benefits. The government also has a strong interest in receiving data to deter, detect, and punish violations of law. Money laundering laws, with their emphasis on "following the money trail," turn out to be at the heart of modern law enforcement demands to have greater access to financial records. More broadly, government access to information holds out the possibility of efficiency gains, not just for law enforcement, but in the overall administration of government.

Part IV examines the possible harms from government access to financial data. Government officials might themselves illegally use personal data, out of self-interest or based on other motives. Hackers and other unauthorized third parties might gain access to the data, especially if many different government officials can extract data from the vault. As suggested by the privacy paradox mentioned above, the political system may make short-term decisions to permit uses of data without giving full consideration to longer-

term and potentially negative effects. Next, in ways not often considered by U.S. policymakers, the adoption of surveillance technologies within the United States may have unforeseen and negative effects on democratic values in other countries. Even where the American legal and political system has sufficient checks and balances to permit use of surveillance technologies, other countries using the same technologies may not. An additional disadvantage of government access may come in the form of bad distributional and discriminatory effects. New accumulations of data may be disproportionately used against the weak by the strong. Finally, the idea of tracing each web page ever visited suggests how free speech and other democratic values may be implicated by new financial or other surveillance technologies. If a society repeatedly opts for surveillance rather than privacy, then the nature of that society may change over time.

This daunting list of possible disadvantages shows why we should take seriously the privacy paradox and the issue of financial privacy. It is also worth recalling, furthermore, how tight the link is between private- and public-sector databases in the financial and other areas. For companies operating in the United States, any information in private hands is only a subpoena away from the government. For companies operating elsewhere, there may be even fewer legal protections against government access. As financial databases develop in the private sector, there is a corresponding increase in the power of government to track each purchase made by individuals.

This Article does not attempt to answer for all places and all times when the government should have access to records of financial transactions. Careful empirical attention is needed in each place and time to weigh the advantages and disadvantages of government access. The identification of advantages and disadvantages in this paper, however, should be useful for the more general task of assessing high-tech government surveillance. This Article questions whether we, as a society, would like the government to have access to the records of every purchase ever made. A closely related issue arises with the growing use of cellular telephones. The government might gain the technical ability to track every move people (or their phones) ever make. As technologies continue to develop, such as toward wearable computers,[2] new realms of data collection will become technically possible (every place visited, every word spoken, and so on). Keeping track of this data will be enormously efficient for many purposes. It will also raise new risks, of the sort analyzed in this Article. Societies will have to determine

2. *See* Wendy M. Grossman, *Wearing Your Computer*, SCI. AM., Jan. 1998, at 46.

how to weigh the tempting advantages of high-tech surveillance with its sobering disadvantages.

I. THE TREND TOWARD TRACEABLE PAYMENTS

At some level, most people understand that the financial transactions of ordinary individuals are becoming more traceable over time. Many transactions are recorded today that did not used to be recorded, or that were recorded only in places that were difficult to find and connect. The spread of computers and computer networks means that data more easily and inexpensively move from one place to another. The result can be accumulation of a detailed dossier about what an individual has purchased. At least potentially, an investigator may uncover an individual's spending patterns over an entire lifetime, gaining incisive and sometimes disturbing insights into the person's personality and actions. In a consumer society, a complete tracking of consumption is very revealing. Concerns about such tracking lead to calls for financial privacy, for some set of rules and institutions that will limit the problems created by our purchases becoming an open book.

This Part explains the differences in traceability as payments move from cash to checks to electronic payments. It then explains reasons why more transactions are becoming traceable over time and introduces some of the categories of harms that can result from such traceability.

A. From Cash to Checks to Electronic Payments

Transactions are becoming more traceable as our society moves from cash to checks to credit or debit cards. Ordinary cash provides the possibility of an untraced transaction. Nothing in the exchange of cash leaves any record linking the purchaser to the purchase. Such a link exists only if some other action is taken to identify the transaction. For instance, the purchaser might fill out a warranty card or some other document, or a video camera may take pictures of a store's customers. Cash transactions may not be anonymous in the strict sense because the sales clerk typically sees the purchaser and may remember the face. A large portion of cash transactions, however, are anonymous in the sense that neither the seller nor any other party can readily link the purchaser to the transaction after the fact.

Payment by check leaves more of a record for the merchant, the banks involved in payment, and the purchaser. Merchants and their clerks can read the name and other information, such as home address, printed on the check. The banks involved in payment keep records in order to credit or debit the

appropriate accounts. The purchaser receives back the checks themselves or records of the checks. In all of these ways there is more of a record than for the cash transaction. That record can become very important if the police or tax authorities investigate the transaction after the fact. At that point, the checks themselves (or pictures of them) can likely be produced. In a cash transaction, by contrast, there is often no record to produce.

In a significant way, credit and debit cards are even more traceable than checks. Historically, banks have usually not created databases for check transactions that listed the payor, payee, and item purchased. For a bank, gathering such information from a paper check would require the large task of entering information about the payor and payee into a computer. By contrast, credit or debit card purchases usually automatically record information about the payor, payee, and items purchased. The merchant's database will often be able to track every purchase made with the same credit or debit card. Even more comprehensively, the credit card issuer will have a record showing the payor, payee, item purchased, date, and purchase price, and so forth. If there is an investigation after the fact, the merchant and card issuer databases can be combined. The card issuer database will identify each place of purchase, and the merchant databases will often allow a detailed accounting of each item purchased (for example, each dish ordered at a restaurant or each prescription filled at the pharmacy).

B. Why More Transactions Will Be Traceable

The shift from cash to checks to credit and debit cards shows an evolution toward creating records, placing the records automatically in databases, and potentially linking the databases to reveal extremely detailed information about an individual's purchasing history. In considering the effects of this evolution on financial privacy, the next issue is the extent to which people will adopt the more traceable means of payment.

A good dose of skepticism is in order before assuming that we will suddenly move to an all-electronic, cash-free society. After all, we are all familiar with the old claims that computers would result in a "paperless office." Few of us, to say the least, work in such offices today. In banking, the history of the automated teller machine ("ATM") provides an instructive guide to how long it can take for new, and seemingly very useful, banking technologies to take hold. It has taken a full generation for users to accommodate themselves to ATMs. Even today, use of ATMs varies widely by age. A 1996 survey showed that only 36% of those above age sixty-four

have an ATM card, compared with 75% of those aged eighteen to thirty-four.[3]

Current payment patterns, moreover, are more heavily weighted toward cash and check payments than most people would suspect. A 1994 study for the Bankers Roundtable reported three hundred billion cash payments per year and fifty-eight billion checks and other paper payments.[4] All electronic-based payments, including debit and credit cards, reached only fourteen billion transactions per year, or less than four percent of the total.[5] Additionally, instead of seeing an abandonment of paper-based technologies, the number of paper checks has continued to rise, albeit at a much lower pace than the number of electronic transactions.[6]

Electronic payments are far more prominent in dollar value than in number of transactions. The Bankers Roundtable study estimated total electronic based payments of about $450 trillion per year (including many large-value business transactions), check and other paper-based payments of $67 trillion per year, and cash payments of only $2.7 trillion.[7] At the consumer level, electronic payments in 1993 accounted for 18% of the number of consumer transactions, an increase from 11% in 1980, with cash at 47% and checks at 31%.[8]

These statistics reflect our status quo, in which large-value transactions and many types of business expenditures are generally made in electronic form. Importantly for the study of financial privacy, however, the large majority of consumer transactions is made by cash and check. These transactions are thus not automatically included in databases revealing individual spending patterns. If consumers use electronic payments more often in the future, as most observers expect, then the status quo will change, to one where records more often will be created, put into databases, and linked to other databases containing personal information. There will be less financial privacy than has traditionally existed in our society.

With the stakes for privacy now made more clear, this Article will explore some of the major reasons to expect that consumers will indeed shift heavily in the coming years toward more traceable electronic payments. New legal

---

3. *See* Valerie Block, *ATM Cards Hit a Wall: The Next Breakthrough Is Years Away, Bankers Say*, AM. BANKER, Jan. 2, 1997.

4. *See* FURASH & CO., BANKING'S ROLE IN TOMORROW'S PAYMENTS SYSTEM 49 (1994).

5. *See id.*

6. *See id.* at 49-54. The number of checks rose seven percent from 1992 to 1993; credit card transactions rose at over a ten percent annual rate from 1983 to 1992; and debit card use has soared from a low base in the 1980s. *See id*.

7. *See id*. at 49.

8. *See id*. at 50.

rules may emerge that encourage or require easily traceable transactions. For instance, the government might ban anonymous payments over the Internet or extend the current rules that require record keeping for cash transactions involving over $10,000. Beyond the effect of new legal rules, consider five market-based reasons why individuals might choose to have a greater proportion of their transactions in an easily-traced form: affinity programs, Internet purchases, security (antitheft) protections, auditing advantages, and electronic benefits programs.

1. Affinity Programs

What would you do to get frequent-flyer miles? What have you already done? One advantage of electronic payments is that the consumer can automatically receive credit in all manner of affinity programs—airlines, rental cars, hotels, grocery stores, cashback programs, and many more. Issuers of electronic payment cards (stored-value, credit, and debit cards) face stiff competition in creating consumer loyalty to their cards. Affinity programs give a reason for consumers to use one issuer's cards again and again. In the context of our discussion, affinity programs also give consumers a strong reason to use electronic payments rather than cash or checks.

2. Internet Purchases

Ordinary green cash does not work over the Internet. Nor does the traditional paper check unless the consumer is willing to wait days until after the check has reached the merchant and been accepted. To date, Internet commerce has been dominated by the fully-traceable credit card.[9] As Internet commerce expands rapidly in coming years, it is quite possible that credit cards and other traceable payment systems will continue to predominate. It is technically possible to conduct strongly anonymous transactions on the Internet,[10] but law enforcement officials have lobbied aggressively against anonymity, arguing instead for escrow of encryption keys and enforcement of money laundering laws. In ways that are less appreciated, even if strong encryption were permitted, there are compelling market and other reasons to expect that the overwhelming majority of financial transactions would not be anonymous.[11] The rise of Internet commerce thus likely brings with it a rise

9. *See* Russell Stevenson, Jr., *Formulating Public Policy for Electronic Commerce*, ELEC. BANKING L. & COMMERCE REP., June 1998, at 16 ("By far the most common type of payment instrument being used by consumers in electronic commerce today is the conventional credit card.").

10. *See* David Chaum, *Achieving Electronic Privacy*, SCI. AM., Aug. 1992, at 96.

11. *See* Swire, *Financial Cryptography*, *supra* note 1 (highlighting the impossibility of lending to

in traceability.

3. Security and Biometrics

If you lose cash, it is gone. If you lose your checks, you may be liable for large amounts. But if you lose your credit or debit card in the United States, you typically are liable only for the first $50 of unauthorized use.[12] Credit and debit cards thus already have a security advantage, which is likely to grow in the future. Credit and debit cards may soon include biometric and other new security measures that will further reduce the risk that someone else will use an individual's card. These measures will also link individuals to their purchases in ways that will be difficult or impossible to deny.[13]

4. Good Audit Trails

For centuries, businesses have known the importance of having a good audit trail. Keeping close track of expenditures helps keep employees honest and eases a multitude of business tasks, including payment of taxes, compliance with internal policies, and planning for optimal expenditures. These advantages of a good audit trail have begun to spread to individuals and families, through financial software such as Quicken. Using cash or checks with such software requires laborious rekeying of the transactions. By contrast, electronic payment information can flow directly into the family database, automatically tracking business deductions, taxable contributions, and other useful categories. Personal financial software will undoubtedly improve over time, creating value-added for consumers as they make payments electronically.[14] Although audit trail systems can in theory be

---

anonymous borrowers, the risks associated with key management of anonymous accounts, and other market acceptance problems for strongly anonymous transactions).

12. *See* 15 U.S.C. § 1643(a)(1)(B) (1994). For an analysis of the different legal rules for unauthorized use of checks, debit cards, and credit cards, see Clayton P. Gillette, *Rules, Standards, and Precautions in Payment Systems*, 82 VA. L. REV. 181 (1996).

13. *See* John D. Woodward, Jr., *Biometrics and the Future of Money*, ELEC. BANKING L. & COMMERCE REP., June 1998, at 1. Woodward argues that biometrics generally will increase security and customer privacy. He admits, however, that the "potential for a breach in database security increases greatly as shortcuts are taken, budgets are slashed, trained personnel are few and leaders do not draft and implement plans to safeguard biometric identification information for which they are responsible." *Id*. at 7. Nothing in Woodward's argument makes these troublesome scenarios seem unlikely.

14. As an example of value-added, consider a patent awarded to Sun Microsystems in 1998, which provides various mechanisms for delivering electronic receipts to an e-mail address, a smart card, or a credit card issuer. *See* Debra Freeman, *Selected Intellectual Property Law Developments*, ELEC. BANKING L. & COMMERCE REP., June 1998, at 19, 21. These electronic receipts might feed automatically into an individual's personal financial software, providing documentation of the

designed to protect the purchaser's anonymity, it is far from clear that widely-adopted systems will do so.

5. Electronic Government Benefits

Affinity programs, biometrics, good audit trails, and Internet purchases may have their greatest effects on the well-off and cyber-savvy. The payments of lower-income Americans will become more traceable for a different reason—the spread of electronic government benefits. Many public-assistance beneficiaries have historically cashed their government checks and paid for everything in cash, leaving little record of individual purchases. New laws will lead to more traceable transactions. For example, the 1996 Debt Collection Improvement Act created a general requirement that after January 1, 1999 Federal Government payments be made by electronic funds transfer.[15] The 1996 welfare reform law required states to convert food stamps from paper coupons to an all-electronic system by 2002.[16] Advantages of electronic payments include lower costs to government, inclusion of lower-income individuals in the mainstream financial system, and likely reduction in fraud. The desire to control fraud, however, may create strong political pressures to have detailed audit trails of beneficiaries' purchases, creating threats to the individuals' privacy.[17]

C. An Anatomy of Harms from Highly Traceable Transactions

The discussion thus far has explained reasons to expect the financial transactions of many individuals to become more traceable. As people use cash and checks less, and electronic transactions more, databases will accumulate information linking the payor, payee, and items sold. In an increasingly networked world, the existence of such databases can easily mean that data will spread from one node to another.

If all of an individual's financial transactions can be traced and are accessible by others, one can envision many possible harms. This Article will not reproduce the large literature showing harms that can arise from

---

expenditures listed in the person's database.

15. *See* 31 U.S.C. § 3332(f)(1) (Supp. II 1996). The Secretary of the Treasury retains discretion to waive application of that requirement for individuals or classes of individuals for whom compliance imposes a hardship or in other circumstances as may be necessary. *See id*. § 3332(f)(2).

16. *See* 7 U.S.C. § 2016(i) (Supp. III 1997).

17. *See infra* Part IV. For one government study recommending widespread use of electronic fingerprint identification as a condition for receipt of government benefits, see U.S. GENERAL ACCOUNTING OFFICE, USE OF BIOMETRICS TO DETER FRAUD IN THE NATIONWIDE EBT PROGRAM (1995).

invasions of privacy.[18] As an introduction to the importance of financial privacy, however, this Article will discuss three examples of invasions of financial privacy: identity theft; the risks posed by having records for every book and web page that an individual reads; and the additional problems created by an authoritarian or totalitarian regime track all financial purchases. With these three illustrations in mind, this Article will then construct an anatomy of harms from surveillance of financial transactions and of high-tech surveillance more generally.

The first example is identity theft, or the assumption of an individual's name for financial gain. As more personal information becomes available over networks, it becomes easier for criminals to get hold of previously-private information. For instance, public birth records (now available from database companies) often reveal a mother's maiden name. State drivers license records, available for law enforcement and marketing purposes, often reveal an individual's Social Security Number. Armed with this information, a criminal can impersonate an individual, get a credit card, and run up large bills under the stolen name. Trans Union, a major credit bureau, reported 350,000 cases of identity fraud in 1997.[19] In the same year, at least 10,000 people were arrested for participating in organized identity theft rings.[20] According to the Secret Service, losses from identity theft soared from about $440 million in 1995 to more than $740 million in 1997.[21] As financial records become more traceable by more people, criminals have greater opportunities to access the records and use them to impersonate innocent victims.

A second problem to consider is government and private-sector access to each book and web page that an individual has accessed. A good deal of public concern accompanied special prosecutor Kenneth Starr's subpoena of the bookstore records of Monica Lewinsky's purchases.[22] To many observers, this subpoena seemed to be a worse invasion of privacy than a

---

18. Perhaps the single best account is in the first three chapters of *Privacy and Freedom.* ALAN WESTIN, PRIVACY AND FREEDOM (1967). Westin identifies the four basic states of individual privacy as solitude, intimacy, anonymity, and reserve. *See id*. at 31-32. Of these, anonymity, or "freedom from identification and surveillance," is most centrally relevant to financial privacy. *Id*. at 31. Westin's broader discussion of the importance of privacy, however, suggests the many social functions of protecting privacy and the many sorts of harms that can result, even for those who comply with laws, if surveillance becomes routine and the area of private space shrinks. *See id.*

19. *See* Jan M. Faust, *Identity Crisis: When Someone Else Becomes You* (visited May 16, 1999) <http://www.abc.com/sections/us/ DailyNews/id_theft981006.html>.

20. *See id.*

21. *See id.*

22. *See, e.g.*, Stephen J. Fortunato, Jr., *In Praise of Susan McDougal*, PRIVACY J., Apr. 1998, at 5-6 (arguing that the bookstore that turned over records of Monica Lewinsky's book purchases could have defied Prosecutor Starr's subpoena on First Amendment grounds). *See id.*

subpoena of other sorts of financial records. The concerns are likely linked to what Professor Julie Cohen has called "the right to read anonymously," the idea that surveillance of reading threatens First Amendment and related free speech values.[23]

That right to read anonymously becomes even more threatened if records are kept for every web site that a user visits. As web browsing becomes a more pervasive aspect of daily life, records of each page visited may provide a startlingly detailed profile of an individual's interests and activities. Depending on how individual users configure their web browsers, personal computers already keep extensive records of what web sites have been visited. Users today have the ability to tell their browser not to retain these sorts of history files.[24] By contrast, users in the future may have less choice about whether to leave traces of their web browsing. Some sites today charge to download desirable content. For instance, USA Today allows free access to same-day articles. Articles from the archive, however, cost $1.00 each, payable by credit card.[25] In coming years, as "micropayment" systems develop that can charge pennies or fractions of pennies per page, such pay-for-content services may become far more common.[26] Unless privacy protections are built in, these payment systems may be fully traceable, allowing after-the-fact access to each web page visited.

The third problem, perhaps even more troubling, is how an authoritarian or totalitarian government might use and abuse information about citizens' financial transactions. Payment technologies developed in the United States are likely to spread to many countries around the world. Some of those

---

23. Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1003-38 (1996). In considering any such right to read anonymously, there are two distinct inquiries. The first is whether courts will accept such a right as a matter of constitutional law. *See id*. at 1003-19. Even if the Constitution does not require such a right, the second inquiry is whether it is good policy for the right to be recognized by statutory or other law. *See id*. at 989-94. Many people, even among those who believe that the Constitution does not provide an enforceable right to read anonymously, recognize that values underlying the First Amendment and the theory of free expression make it especially worrisome for governments to be able to track every item read by citizens.

24. *See* Carole Lane, *Going Private: How to Protect Yourself from Hackers, Snoops, and Spammers*, PC WORLD, Sept. 1, 1998, at 115.

> Web browsers do a great job of helping you return to frequently visited sites by keeping a running list of where you've been. Unfortunately, anyone who has access to your system—your boss, your family, the janitor—can scrutinize which Web sites you've been favoring by cruising through your browser's history list. If you don't want anyone else to know where you've been and what you've seen, you need to clean up after yourself. But it's not easy.

Id. at 118-23.

25. *See USA Today* (visited Mar. 20, 1999) <http://www.usatoday.com>.

26. *See* A. Michel Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COMM. 395 (1996).

countries lack the democratic history and judicial oversight that exist in the United States. Dictators and other officials in these countries might be able to track the financial transactions of ordinary citizens and political opponents. Surveillance technology that we might find acceptable in the United States, due to a well-functioning system of checks and balances, may be unacceptable in other countries.

These examples suggest the range of problems that can result from the tracking of financial transactions: security breaches due to widespread availability of personal information (identity theft); threats to free speech and other values when a wider scope of activities are traced by new technology (web browsing); and the increasing severity of problems when judicial and political checks on surveillance are eroded (police state). The discussion in Part IV will describe other disadvantages that can arise from tracking of financial transactions.

For each of these problems, one can identify four types of costs from surveillance: (1) the harms themselves, such as losses caused by theft, revelation of embarrassing information, or persecution by a corrupt regime; (2) chilling effects, or activities foregone due to surveillance; (3) cloaking costs, or actions taken to evade surveillance; and (4) burdens of having to comply with surveillance requests. The focus here is on the burdens that arise from surveillance. Weighing those burdens against the benefits of surveillance will be discussed later in the Article.

1. The Harms Themselves

The first and most obvious concern is for direct harms resulting from surveillance. For identity theft, the existence of traceable transactions means that the criminal can more easily seize personal data and use the information for fraudulent purposes. Victims may have to pay credit card bills that were incurred by others.[27] Often even more burdensome, victims may undergo considerable time, expense, and mental distress in disputing such bills and cleansing personal credit histories.[28]

Disclosure of web browsing might create any number of harms. People may look at many things on the Internet that they would not publicly broadcast. Pedestrian examples include the many people who visit

27. Under U.S. law, a customer's loss from unauthorized credit card use is typically capped at fifty dollars. *See* 15 U.S.C. § 1643(a)(1)(B) (Supp. II 1996). There are, however, circumstances when customers may pay for unauthorized charges, such as when they do not notice unauthorized purchases on their bill or when they find it easier to pay the bill than dispute it.

28. *See* Michael Higgins, *Identity Thieves*, J.: LAW. MAG., Oct. 1998, at 42 (discussing losses caused by identity theft).

pornography and gambling sites. Gay, lesbian, or bisexual people might have their sexual orientation revealed. Women who seek information on having an abortion might be tracked. Visitors to political web sites could be identified. The web records would show who reads about embarrassing medical conditions, from impotence to incontinence to any other condition that people might not wish revealed. For people in business, the pattern of web reading might be of economic value to competitors—why is so-and-so reading about that topic? For families, web searches about substance abuse, psychological problems, or other topics might reveal sensitive information to neighbors, employers, or public officials.[29] Such examples could be multiplied.

In debates about privacy and surveillance, those favoring disclosure sometimes suggest piously that only criminals or others with something serious to hide should care about privacy. In this list of possible harms from disclosure of web browsing, all of the activities revealed are legal. Law-abiding people can suffer real harms from disclosure of personal information.

The harms from surveillance of all financial transactions are even easier to imagine in a police state. In the absence of effective checks on official power, those in control might use the information for their economic or political advantage. Political opponents, disfavored minorities, and powerless people generally could be targeted for exploitation by government officials.[30]

2. Chilling Effects

If I know that I am under surveillance, I might be able to prevent the sorts of harms just discussed. A chief way to do so would be to restrict my activities, so that nothing embarrassing or otherwise harmful could be detected. This "chilling" effect on activities is one of the most widespread results of surveillance. As discussed in Part III below, the chilling or deterrence effect reduces crime and other antisocial behavior, and is thus a major justification for creating surveillance systems and limiting privacy. This section suggests how surveillance can also chill or deter desirable behavior.

In looking to the above three examples, a high risk of identity fraud would tend to chill activities that result in identity fraud or are perceived to

29. For a somewhat similar set of examples, on which this list is loosely based, see ANN CAVOUKIAN & DON TAPSCOTT, WHO KNOWS: SAFEGUARDING YOUR PRIVACY IN A NETWORKED WORLD 13-14 (1997).

30. The harms potentially caused by powerful officials are discussed in greater detail below. *See infra* Part IV.A.

result in identity fraud. For instance, consumers who are concerned about the safety of transmitting their credit card numbers over the Internet will tend to avoid Internet purchases. More generally, concerns about identity theft might prompt individuals to use less traceable means of payment, such as cash, even when they would otherwise prefer to use credit cards or other more traceable means of payment.

The chilling effects could be widespread and significant if government gained the power to track every book and web page read by an individual. The United States Supreme Court has upheld the right to write anonymous political pamphlets, recognizing the chilling effect on speech if authors must be identified.[31] In the 1997 case striking down the Communications Decency Act, the Supreme Court appreciated the chilling effect that vague and overbroad restrictions on pornography would have on free expression on the Internet.[32] And, as mentioned above, Professor Cohen has made important arguments about how free expression might be chilled by surveillance of what individuals read.[33]

The chilling effects of tracking web browsing are not limited to traditional First Amendment concerns about free expression in writing, speaking, and reading. Surveillance of financial records and web browsing may chill activities that have only a modest expressive dimension—medical concerns, business activities, or hobbies that one might find embarrassing. Such activities might not win constitutional protection under the First Amendment, but are nonetheless highly desirable. Faced with the knowledge that every web search might be tracked, people would have reason to refrain from any browsing that they would not wish to have generally known. At the limit, the surveillance may approach that found in the "total institutions" studied by Erving Goffman, such as a jail or military base, where the knowledge that one is being constantly watched can change behavior and impose a heavy psychological burden.[34]

Turning again to the example of the police state, the chilling effect of surveillance can be pervasive. In a totalitarian regime the individual does not feel free to go against the wishes of the state. Personal expression and freedom of action are chilled by the fear of detection and punishment.

---

31. *See* MacIntyre v. Ohio, 514 U.S. 334 (1995).
32. *See* Reno v. ACLU, 521 U.S. 844 (1997).
33. *See* Cohen, *supra* note 23, at 983-89.
34. *See* ERVING GOFFMAN, ASYLUMS: ESSAYS ON THE SOCIAL SITUATION OF MENTAL PATIENTS AND OTHER INMATES (1961).

3. Cloaking Costs

As surveillance mounts, people may make greater efforts to hide, or "cloak," information that they wish to keep private. In the physical world, people might pull a cloak up to cover their face from an onlooker or a surveillance camera. Military aircraft use cloaking or stealth technology to become invisible to radar. As the aircraft example suggests, these cloaking costs may be substantial.[35]

One would expect to see similar cloaking costs as recordkeeping and the possibility of detection increases for financial transactions. To reduce the risk of identity theft, people might take the trouble to act untraceably by using cash or pseudonyms. A person scared to use a credit card for a telephone or Internet purchase might instead take a taxi across town to pay in cash. The additional time and expense of going across town are "cloaking" costs. As an example of using a pseudonym, people might do business through wholly-owned corporations rather than in their own names. Expenses of creating the corporation, and acting through it in ways that are difficult to trace, are cloaking costs. It is rational to incur cloaking costs up to the point where the expected benefit of the cloaking exceeds the expected cost from identity theft or other harm.

Similar cloaking costs might be incurred to avoid leaving traces of web browsing. For instance, people might do potentially embarrassing browsing from a public terminal, in a library or cafe, rather than from their own computer. The public terminal acts much like the traditional pay telephone, which can be used to make untraceable calls. Embarrassing browsing might also be done using a borrowed, stolen, or otherwise untraceable Internet account. These sorts of countermeasures may evade surveillance, but they impose cloaking costs on those who do not wish to have their activities observed.

The motivation for cloaking is particularly easy to understand in a police state. Where the individual mistrusts the state and the state has broad surveillance powers, the individual may take extraordinary measures to hide economic or other activity.

4. Burden of Complying with Surveillance

Even when an individual's other activities are not affected, complying

35. The cost of each B-2 stealth bomber, for instance, is about $2 billion. *See* Steven Komarow, *Desert Thunder Plan of Attack: Waging War Was Simpler, Victory More Clear Cut*, USA TODAY, Feb. 13, 1998, at 1A.

with a surveillance system can impose burdens. Consider the growing practice of requiring fingerprints from those who wish to cash a check at a bank. There may be minimal risk of harm to the individual from providing a fingerprint, in the sense that good protections may be in place against anyone stealing the fingerprint. The chilling effect, on those who will cash checks anyway, may be small. As for cloaking effects, presumably few people will try to fraudulently reproduce another's fingerprints. Nonetheless, even if these types of harms are nonexistent, and even if the process is quick and clean, some individuals will experience the fingerprinting as burdensome. Some people will feel a sense of personal invasion, of stigma, at being printed like a criminal. Others may be saddened by the loss of trust or community in society that the fingerprinting represents. Still others might worry about what will be done with the fingerprints, even if good measures are in place to prevent misuse.

Returning to the three examples, new burdens may result from the growing incidence of identity theft. Over time, because mothers' maiden names and Social Security Numbers are becoming less secure, society will have to develop new methods for establishing identity.[36] These new methods may make the mechanics of a transaction more burdensome. Some methods of secure digital signatures, for instance, make an Internet transaction take substantially longer than the current, and less secure, use of credit card numbers.[37] The new methods may also require use of fingerprints or other biometric techniques to establish identity. As with use of fingerprints in cashing a check, some people will feel an invasion of privacy and loss of autonomy from having to participate in such a system.

In the case of web browsing, the burden of complying with surveillance may be small or nonexistent. Indeed, tracking a person's web purchases may be automatic and unobserved by the user, just as collection of "cookie" information often is today.[38] On the other hand, the burdens may be significant. There may be web sites, which a user very much wants to use,

---

36. A mother's maiden name often appears on a person's birth record as the middle name of the mother. Because birth records are generally treated as public records in the United States, and public records are increasingly available from on-line companies, it is often possible to learn a mother's maiden name. As for Social Security Numbers, many states use SSNs in their drivers' records, and these records are often available to direct marketing and other companies.

37. *See* John D. Muller, *Selected Developments in the Law of Cyberspace Payments*, 54 BUS. LAW. 403, 407-08 (1998).

38. Cookie technology allows a web site to place bits of code, or "cookies," on a user's hard drive. The code permits tracking of information about where a user goes on the web site itself, as well other information about the user's operating system and browsing activities. For steps users can take to counteract cookies, see *Anti-Cookie Measures* (visited Feb. 21, 1999) <http://www.junkbusters.com/links.html#measures>.

that condition access to the site on the supplying of detailed personal information.[39] It is also possible that users in the future will need to get the equivalent of drivers' licenses in order to browse on the Information Superhighway.[40] If these licensing procedures become widely-used, there will be the burden of applying for such licenses, as well as the perception of a burden from having one's movements tracked.[41]

The burden of complying with surveillance is especially easy to see in a police state. In the physical world, there is the oppressive need to hand over one's papers at every police checkpoint. For financial transactions, the state might require forms to be filled out or other actions to be taken that constantly remind individuals of the presence of surveillance.

II. WHERE DOES THE DATA GO—THE VAULT 600 FEET DOWN

Part I of this Article explained the reasons for believing that financial transactions will be increasingly traceable over time. It also began to explore why such traceability may be a problem. Significant harms can result from security breaches (identity theft), from the way that disclosure of financial records can threaten free speech and other values (web browsing), and from the power that control over information can give to authoritarian and totalitarian regimes (police state). Part I also provided an anatomy of harms from invasions of financial privacy and from surveillance more generally: the harms themselves; the chilling effects, or actions foresaken due to surveillance; the cloaking effects, or actions taken to evade surveillance; and the transaction costs and emotional burdens of complying with a surveillance system.

---

39. For some sites, the user may not feel there is really any choice whether to use the site. For instance, an employer might condition payment of benefits on providing information via its site, and a monopoly public utility might condition service on receiving information via its site. For other sites, the user might perceive a net gain from going to the desirable site but may nonetheless begrudge the need to provide information. In economic terms, the consumer surplus from the transaction is still positive but is reduced by the burden of complying with the requests for information.

40. For an interesting novel that makes the requirements of such licenses an important theme, see MELISSA SCOTT, TROUBLE AND HER FRIENDS (1994). The novel also employs the helpful term "syscops" to refer to the "system cops" who are responsible for ensuring that their computer systems are in compliance with legal rules. *See id*. at 56-65 (explaining one such investigation by these syscops).

41. For a contrast of the desirability of such licensing approaches for access to adult content to approaches based on the use of filters, see Lawrence Lessig & Paul Resnick, The Architectures of Mandated Access Controls (Sept. 8, 1998) (unpublished manuscript, available at <http://www.si.umich.edu/~presnick/papers/lessig98/> (visited June 20, 1999)). If web purchases rely on the use of certificate authorities to authenticate the purchaser's identity, then there will be a similar burden for purchasers to apply for the certificates. *See* Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996).

All of these harms, and others discussed below in Part IV, may result from increased traceability of financial transactions. In considering financial privacy, however, harm to individuals depends crucially on how the data are used and misused; harm does not depend on the mere existence of data. As a logical matter, the creation of a database does not mean that damage will be done to individuals' privacy. Damage may result as data emerge from the database and are used in particular ways.

A. The Vault 600 Feet Down

A thought experiment makes this point easier to grasp. Imagine that all of the data about an individual's transactions flow into a database. The database is in a super-strong vault 600 feet beneath the Earth's surface. By the terms of the thought experiment, data can flow into the vault but cannot flow out.[42] Once the database is created, the data simply sit there until the end of time. If the vault is truly tamper-proof, then no harm to privacy will result from leaks of the data.[43]

In real life, of course, there is no such foolproof vault 600 feet down. Even if such a vault were proposed, for instance, worries might exist about whether those who constructed the vault had built a "back door" into its hardware or software, allowing later entry by the workers or their associates. Nonetheless, a surprisingly good simulation of the vault might exist in the form of the data centers operated by some of the largest credit card issuers. These data centers, sometimes operated in remote locations, have high fences and other strong physical security. They have (or should have) security specialists who guard against unauthorized access to data by both employees and outsiders. And they have (or should have) substantial computer staffs to assist the specialists provide virtual security against crackers.

B. Why the Vault Metaphor Is Useful

The image of a vault 600 feet down (or the real-life data centers) helps

---

42. It is intriguing to think about how to make the vault truly tamper-proof. The vault might, for example, explode if anyone ever tried to enter it. For one science fiction account of an apparently foolproof vault, see DAN SIMMON, ENDYMION (1996).

43. At least two further assumptions would be necessary to assure no harm to privacy interests. First, transfers of data into the vault must be secure. That is, the data must travel from the transaction to the vault without interception by outside parties. Second, individuals must perceive the vault and transfers to the vault as secure. If individuals mistakenly believe that the data will be used in harmful ways, then their participation in the transactional system might be chilled. In such circumstances, worries about privacy would prevent individuals from entering into transactions they otherwise would have chosen.

focus our attention on exactly how financial data might escape out to the surface of the world. We can imagine each use of data as a pipeline going from the vault to the surface. Some pipelines might lead only to other highly secure locations, where the data will be used for admirable reasons. Suppose, for instance, that the financial data only would be used to catch high-level, dangerous criminals. In such circumstances, most people would agree that the benefits of having the pipeline outweigh the risks to privacy. Other pipelines, however, might create large and unjustified risks to privacy. Suppose, for instance, that the pipeline led to a site that automatically posted all of the transaction records of individuals onto the web. In such circumstances, a similar majority would conclude that the risks to privacy outweighed the benefits of having the pipeline.

The vault metaphor focuses attention on whether it is desirable to allow the intended recipients to have the data. What are the legitimate uses of data by that category of recipients? What risks, to privacy or otherwise, accompany each of these uses? Focusing first on the use of data by the intended recipients themselves, we can ask whether this sort of pipeline is worth constructing.

The metaphor also helps us visualize an analytically distinct problem—access to data by unauthorized third parties ("UTPs").[44] The metaphor helps show two different ways that UTPs might get the data. First, the pipelines to the surface might be tapped by malicious third parties. If there are many pipelines (many withdrawals of data from the vault), then hackers will have many targets for grabbing data en route to the intended recipients. Fortunately, good encryption and other security practices can often make this risk manageable. Second, and more importantly, the data may not be secure once they reach the intended recipients on the surface. Previously, the data were housed in an impregnable vault 600 feet down; now they might be sitting in a "flimsy shack" on the surface. The data transported out of the vault will only be as secure as the flimsiest of these shacks. The risk to privacy is especially great in our modern age when each computer that receives data from the vault can generally make instant and multiple copies of that data and disseminate the data widely over networks. If a burglar enters one flimsy shack, the burglar can copy and spread all the data accessible from the shack's computer.

One caveat is needed about the metaphor of the single enormous vault, 600 feet down. Everyone knows that there has been a change over the past

---

44. The first two parties are the individual data subject and the organization operating the vault. The intended recipients are authorized third parties. Hackers and others who get the data are unauthorized third parties.

few decades in computer technology, from a centralized pattern of a few mainframe computers to the distributed processing model of today's Internet.[45] This shift to distributed processing might seem to contradict the metaphor of a single vault. I suggest, however, that the vault image is nonetheless highly useful. Credit and debit card transactional data are likely to flow into one or a few major data centers, often operated by or on behalf of the card issuer. Instead of one vault holding the data, there might be a few with records of a particular transaction. The key question still arises, however, about what pipelines should emerge from any given vault—who should be able to access the data? Many of the other important categories of surveillance data are similarly likely to be collected in a small number of data centers: tax returns with the IRS, records of telephone calls with large telephone companies, and records of the location of a cellular phone with large telephone companies. In some instances, subsets of these records will exist in other data centers, such as when a merchant can link some customers to their credit card numbers. These other databases, however, will not be nearly as comprehensive as those in the major data centers, and will consequently be less useful to government surveillance. For analytic purposes, we can discuss what rules are appropriate for the government receiving data from one vault. As discussed below, the risks to privacy will be higher to the extent data is housed in multiple vaults. Anonymity will then be a more compelling option.

C. Who Gets the Data, Good Procedures, and the Anonymity Option

A complete analysis of financial privacy requires careful attention to how types of data flow into and out of the vault. Some of the pipelines out of the vault will be to governments. Such uses of data help law enforcement, but may also lead to a range of undesirable uses of government power. Part III of this Article sets forth the arguments for government access to financial data. Part IV similarly examines the arguments for limiting such government access.

Some of the pipelines out of the vault flow to authorized users in the private sector. Credit card companies, for instance, might use the data as part of a fraud protection program[46] or might release the data, when legal, to

45. An entire chapter of my recent book explores the implications for privacy regulation of the shift from centralized mainframe processing to distributed processing over a network. *See* SWIRE & LITAN, *supra* note 1, at 50-75.

46. For example, a few years ago Citibank ran a series of television ads touting its fraud protection program, which contacted the customer for verification when a "jeans sort of guy" got married and started to charge champagne and other luxuries to his credit card. In this example, the data

affiliates for marketing purposes. Such private-sector use of data is the "data protection" issue that is the primary subject of the European Union Directive on Data Protection, which took effect in October 1998.[47]

Finally, some of the pipelines out of the vault might flow directly to unauthorized third parties, who may have found a vulnerability in the vault's defenses. More likely, however, these unauthorized third parties will tap into other pipelines or will grab the data from authorized recipients. Recently proposed legislation would address this problem in part by making it a federal crime to use false pretenses to gain someone's financial information.[48]

In considering all of the possible government, private-sector, and unauthorized uses of financial data, one sees how far we have traveled from the initial thought experiment. Originally, the data were locked securely and permanently in an inaccessible vault. Now, the image shifts to that of the New York City water system—untold thousands of miles of pipes leading in every direction, with large and unstoppable leaks bursting out in innumerable places. The reality of financial data flows, I hope and believe, is much more watertight than New York's aging water system. The analysis below of uses of financial data is intended to help understand where and how leaks or other misuses of data are most likely to occur.

There are two main policy responses as data flow out of the vault and into this potentially leaky system. The first is to create good procedures. Good rules and operating practices would limit when data leave the vault and assure the security of data that do go to the surface. When good procedures are not available, the second response is to prevent data from entering the vault in the first place. For transactions where the privacy risks outweigh the advantages of data flows, that means allowing or encouraging the option of anonymity.

1. Procedures for Protecting Data Leaving the Vault

One general method for controlling leaks is to institute strict procedures whenever data leave the vault. In the United States, the rules concerning these procedures are usually called "privacy" or "data privacy" laws, while Europeans more often refer to them as "data protection" laws. In Europe, national laws seek to control use of data in government and the private sector, and the European Union Data Protection Directive creates

---

on past purchases created an alert when the pattern of purchases changed.

47. *See* SWIRE & LITAN, *supra* note 1, at 102-21.

48. *See* H.R. 4321, 105th Cong. § 2 (1998); S. 2433, 105th Cong. § 2 (1998).

harmonized rules for mainly private-sector processing of personal information.[49] In the United States, the Privacy Act of 1974 sets somewhat similar rules for how the Federal Government can handle data about citizens.[50]

Under the U.S. Constitution, one might suppose that bank records would be accorded some protection under the Fourth Amendment's prohibition against unreasonable searches and seizures. As discussed in this Article, unlimited access to financial records could lead to abuses of governmental power, of the sort historically targeted by the Fourth Amendment. The Supreme Court, however, has thus far rejected constitutional claims to the privacy of financial records held by banks. In the leading case of *United States v. Miller*,[51] a bank customer claimed a Fourth Amendment interest in microfilm records of checks, deposit slips, and other records relating to his accounts at two banks.[52] The customer claimed that these records were within his expectation of privacy and should not be provided to the government in a criminal enforcement action.[53] The Supreme Court denied the customer's claims, holding that the materials were the business records of the *banks*, and not the customer's private papers.[54] Essentially, the individual had waived any expectation of privacy by voluntarily doing business with the bank in a manner that would reveal his financial activities to bank personnel.[55]

Where privacy rights are not recognized as a matter of constitutional law, Congress or state legislatures can create such rights by statute. In the wake of *Miller*, Congress enacted the Right to Financial Privacy Act of 1978 ("RFPA"), which protects customer records maintained by certain financial institutions from improper disclosure to officials or agencies of the Federal Government.[56] Disclosures may be made only where authorized, such as through written customer authorization, subpoenas, search warrants, and formal written requests.[57] With narrow exceptions, customers must be notified in advance before the financial institution releases their records, and

---

49. For a discussion of the Data Protection Directive, see generally SWIRE & LITAN, *supra* note 1, at 28-33.

50. *See* 5 U.S.C. § 552a (1994).

51. 425 U.S. 435 (1976).

52. *See id*. at 437-39.

53. *See id*. at 442.

54. *See id*. at 442-43.

55. *See id*. at 443.

56. *See* 12 U.S.C. §§ 3401-3422 (1994). For a detailed treatment, see 1 L. RICHARD FISCHER, THE LAW OF FINANCIAL PRIVACY ¶¶ 2.01-2.10, at 2-1 to 2-130 (3d ed. 1998).

57. *See* 12 U.S.C. § 3402 (1994).

the customer is given an opportunity to object to release.[58]

The RFPA suggests both the potential and limitations of the statutory approach to privacy protection. The potential is that the RFPA establishes fairly detailed procedures before federal officials can gain access to bank records. In this respect, the RFPA is similar to other statutes that create procedures governing Federal Government access to wiretaps and other defined electronic communications,[59] cable television records,[60] and video tape rental or sale records.[61]

The limitations of the statutory approach are suggested, first, by the rather short list of circumstances where procedures are required before data about individuals, in the hands of other parties such as businesses, can be supplied to the Federal Government. Under the RFPA itself, moreover, only the Federal Government must follow the procedures, including notice to the customer, before seeing the records. State and local governments are exempt from the requirements of the Act, (unless a separate state law exists) as are private organizations.[62] The Act has also been read to have other exceptions, such as where an Internal Revenue Service summons was held valid despite its noncompliance with the requirements of the Act.[63] Furthermore, even where statutes require good procedures, there is the additional empirical question of the extent to which the government follows the procedures. Many Americans would hope and believe that government officials in the United States follow legal requirements before obtaining records. In some other countries, however, there would be heightened concerns about whether officials are scrupulous, even where legal restrictions on access exist.

2. The Anonymity Option

At least as a matter of theory, good procedures created by statute can be a sufficient answer to concerns about government access to personal financial information. One can imagine a well-crafted set of laws and regulations that calibrate the level of required procedure to the privacy risk in each setting. In

---

58. *See id.* § 3409. Along with other requirements, delayed notice is permitted only if

> there is reason to believe that notice will result in—(A) endangering life or physical safety of any person; (B) flight from prosecution; (C) destruction of or tampering with evidence; (D) intimidation of potential witnesses; or (E) otherwise seriously jeopardizing an investigation or official proceeding or unduly delaying a trial or ongoing official proceeding.

Id. § 3409(a)(3).

59. *See* 18 U.S.C. §§ 2510-2511 (1994 & Supp. III 1997).

60. *See* 47 U.S.C. § 551(h) (1994).

61. *See* 18 U.S.C. § 2710(b)(2) (1994).

62. *See* 18 U.S.C. §§ 3401(3), 3402 (1994).

63. *See, e.g.*, United States v. MacKay, 608 F.2d 830 (10th Cir. 1979).

the real world, however, such a well-crafted system might not exist. The privacy-protective laws might not be enacted; if enacted, they might not be followed by officials.

The next question, then, is what should be done when the pipeline system leaving the vault is fatally flawed, when the privacy and other disadvantages of having data leave the vault outweigh the advantages of sending the data up the pipelines. The answer, in such circumstances, can be to prevent the data from entering the vault in the first place. When there are inadequate controls on data that leave the vault, then one might have filters on flows *into* the vault.

For transactions with high privacy risks, that means allowing the option of anonymity. As a start, we might design systems that minimize the number of parties who can access the data before it flows into a secured vault. For example, one problem with credit card transactions today is that the merchants and the merchants' banks see the credit card number of the purchaser. A waiter in the restaurant or a web site operator can copy down the account number and use it in unauthorized ways. One way to reduce this problem is to implement the SET or other new credit card protocols that hide the account number from the merchant and the merchant's bank. In such systems, the transaction can be traced only by the individual buyer and the buyer's bank. In this way, the buyer's account number is filtered out of the merchants' databases, reducing the risk to security and privacy.

More thorough anonymity is also possible. Internet payment systems are technically feasible that would have the purchaser's bank also be unable to link the transaction to the individual purchaser.[64] In some of these systems, the purchaser's identity would indeed become known to the purchaser's bank, but only in specified circumstances, such as where the purchaser defaulted on a payment.[65] With the development of new payment systems and other new technologies, system designers and policymakers have many choices on the spectrum between complete traceability and complete anonymity.[66]

In concluding the discussion of the vault, it is now easier to see the fundamental choices for structuring flows of personal information. Information can be filtered out before it reaches the vault. In such cases, as in today's ordinary cash transactions, there is anonymity in the sense of not creating a data link between the individual and the transaction. Once the data

64. *See* Chaum, *supra* note 10, at 96.

65. *See id.*

66. See the many thoughtful essays in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE (Philip E. Agre & Marc Rotenberg eds., 1997).

enters the vault, it might be left there forever untouched, deep under the ground. Or the data might flow to the surface through various pipelines. Legal rules and good operating procedures can provide security for the data while in the pipeline. Other good rules and procedures can limit who can access the data once it reaches the surface. For each pipeline, we can assess the advantages and disadvantages of allowing data to come to the surface.

III. ADVANTAGES OF GOVERNMENT ACCESS TO TRANSACTIONAL INFORMATION

The vault analogy can be used to visualize the risks and benefits of information-gathering systems both for financial and for other data, such as tracking of cellular phones or key escrow of encrypted messages. The discussion in this Part will examine the advantages of government access to records of the financial transactions of individuals. Subsequent Parts explore the disadvantages of such access and the ways the analysis can be generalized to assess government surveillance in other settings.

The government has a strong interest in receiving data relevant to its own financial affairs, such as collection of taxes and distribution of benefits. It also has a strong interest in receiving data to deter, detect, and punish violations of law. These two interests combine in enforcement against tax evasion and benefits fraud. Along with this criminal and civil enforcement, money laundering laws, with their emphasis on "following the money trail," turn out to be at the heart of modern government demands to greater access to financial records. More generally, government access to information holds out the possibility of efficiency gains, not just for law enforcement, but in the administration of government more generally.

A. Financial Affairs of the Government Itself

The government receives considerable financial information from individuals when the government itself is a party to the transaction. Some of these transactions involve payments to the government, such as taxes. Some of them involve payments from the government, such as welfare and other transfers to low-income beneficiaries.

There are compelling reasons for the government to receive accurate financial information for these transactions. As a general matter, parties to a transaction often insist on detailed and accurate financial information. Private-sector mortgage lenders, for instance, typically insist on verifying a great deal of information about the borrower. For the government, when collecting taxes, access to financial records helps correct for the sometimes

overwhelming human temptation not to pay all of the taxes due by law. On the benefits side, accurate information reduces the likelihood that people will fraudulently or mistakenly receive benefits for which they are not eligible.

Where the government's own money is at stake, the case for access to financial information is easily grasped. Accurate financial information makes the administration of tax and benefit programs more efficient. Such information helps uphold the rule of law in government financial transactions. By treating like cases alike, good information helps achieve fairness and the perception of fairness. A perception of fairness, in turn, likely increases citizen compliance with tax and eligibility rules.

These arguments, although powerful, are limited by their rationale. They explain why the government, much like a private lender or other party, should have access to the information required for its own financial transactions. The arguments do not give a reason, however, for the IRS or a benefits office to share information with agencies that do not need the information to assist in the government's financial affairs.

B. Laws to Detect, Deter, and Prove Illegality

A more general reason for government access to financial information is to assist in enforcement of the laws. There is a long and distinguished history, for instance, of requiring good records to prevent fraud. The Statute of Frauds, passed in England in 1677, required that important contracts be memorialized in writing.[67] Under U.S. securities laws, an issuer must provide detailed written disclosures of all material facts.[68] If disputes later arise about what issuers promised, disgruntled investors can introduce the writings in court and thereby prevent issuers from changing their story.

Financial records can be extremely useful in detecting a variety of illegal behavior. For instance, discrepancies in financial records can uncover embezzlement and other illegal acts. An important role of outside auditors is to scrutinize the records of transactions in order to uncover such problems. This possibility of detection, in turn, serves as a deterrent to crime. Employees are far less likely to steal if they know that internal records, checked by outside auditors, will leave a record of their criminality long after the crime is committed. Furthermore, a party can use detailed records in court

---

67. *See* JOHN D. CALAMARI & JOSEPH M. PERILLO, THE LAW OF CONTRACTS § 19-1, at 774-75 (3d ed. 1987). For example, to enforce contracts for land or for longer than one year, courts ordinarily required the contracts to be in writing. *See id.*

68. *See, e.g.*, 15 U.S.C. § 77k (1994) (creating civil liability for false registration statements); *id.* § 78j (forbidding "in connection with the purchase or sale of any security . . . any manipulative or deceptive device").

after the fact to prove the existence of illegal behavior.

One can therefore see how detailed financial records can further the central goals of law enforcement, namely, the detection, deterrence, and proof of illegal activity. The historical pattern has been to permit law enforcement officials to obtain financial records where they exist, often by means of a subpoena, warrant, or other legal process. The historical pattern for certain limited categories of transactions has been to require a writing, such as for the issuing of securities or for contracts covered by the Statute of Frauds. Until recently, however, law enforcement officials have not made it a priority to require that ordinary transactions leave permanent records.

C. Money Laundering Laws and Privacy

The possibility of mandated records becomes far more likely in the context of modern money laundering laws. According to the U.S. Financial Crimes Enforcement Network ("FinCEN"), money laundering laws are essential to the government's ability to "follow the money trail." U.S. money laundering laws today apply to large transactions. A "currency transaction report" ("CTR") must be filed with the government for cash transactions over $10,000.[69] Similar forms are required for the import or export of over $10,000 in currency.[70] Related rules prohibit "structuring" smaller transactions in order to avoid the $10,000 trigger for reporting requirements.[71] Banks and other institutions also must institute various "know your customer" practices. Notably, existing regulations require banks to file "suspicious activity reports" for situations such as where the

> transaction has no business or apparent lawful purpose or is not the sort [of transaction] in which the particular customer would normally be expected to engage, and the institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.[72]

Money laundering rules have been expanded repeatedly in recent years,

---

69. For an extremely detailed treatment of current money laundering laws, see FISCHER, *supra* note 56, ¶¶ 4.01-4.13, at 4-1 to 4-101. For regulations on Currency Transaction Reports, see 31 C.F.R. § 103.22 (1998). For discussion of CTR requirements, see FISCHER, *supra* note 56, ¶ 4.06, at 4-25 to 4-50.

70. *See* 31 U.S.C. § 5316 (1994); 31 C.F.R. § 103.23(a) (1998).

71. *See* 31 U.S.C. § 5324. The structuring rules were enacted as part of the Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207-18, as were provisions allowing for the forfeiture of assets obtained or used by money launderers. *See* 18 U.S.C. § 981(a)(1) (1994).

72. 12 C.F.R. § 21.11(c)(4)(iii) (1998). This regulation was promulgated in 1996. *See* 61 Fed. Reg. 4337 (1996). A 1998 proposal to expand the "know your customer" rules is discussed below.

both in the United States and other countries. A seemingly inexorable logic has underlaid this expansion. The original trigger of a $10,000 cash deposit created incentives to make deposits of $9,999, leading to passage of the "structuring" laws. As banks began to keep stricter records, the temptation grew for criminals to use other institutions, such as casinos, as the preferred route for laundering cash. The result has been a steady expansion of the range of institutions covered by the reporting requirements.[73]

The next horizon for money laundering experts is to assure that similar rules apply to electronic cash transactions. This view is well expressed by noted criminal law professor Sarah Welling, who with coauthor Andy Rickman has recently written an article entitled *Cyberlaundering: The Risks, The Responses.*[74] The authors have worked extensively with Fincen, and their central point is clear: "The government must be able to trace transfers of value to detect and prosecute money laundering."[75] In connection with the rise of traceable payments, the authors are explicit: "The government should require the issuers to design the electronic cash systems to create an audit trail."[76] That is, the money laundering enforcement community believes that untraceable electronic transactions should be forbidden. Otherwise, enforcement officials fear a giant loophole will emerge in the current system of money laundering laws.

In Welling and Rickman's detailed article on cyberlaundering, the entire topic of privacy receives only a single sentence: "Privacy interests of consumers and merchants often will conflict with the government's interest in obtaining information to prevent money laundering."[77] This extremely brief attention to privacy concerns has been common thus far among those involved in money laundering enforcement. Based on my own interviews with U.S. prosecutors and others involved in money laundering enforcement, there was no substantial intellectual or political pressure until 1999 to explain how to reconcile privacy concerns with the rapidly-expanding web of money laundering laws. Until recently, enforcement officials have been supported in this attitude by the mainstream political community in the United States, which has viewed money laundering laws as a popular component of the war

---

73. See FISCHER, *supra* note 56, ¶¶ 4.02-4.03, at 4-10 to 4-17.

74. Sarah N. Welling & Andy G. Rickman, *Cyberlaundering: The Risks, the Responses*, 50 FLA. L. REV. 295 (1998).

75. *Id*. at 320. The article itself grew out of the authors' participation in conferences jointly sponsored by FinCEN and the Rand Corporation. *See id*. at 295 nn.a1-aa1.

76. As another component of a thorough system of money laundering rules, the authors state that "the government . . . needs to be able to decrypt these messages when criminal activity is suspected." *Id*. at 322.

77. *Id*. at 317.

on drugs, and not as a threat to the privacy interests of ordinary citizens.

As of early 1999, there are important signs that this political calculus is beginning to change. The first wave of opposition to money laundering regulation emerged in connection with the U.S. Government's campaign for mandatory key escrow for cryptography. Under the "Clipper Chip" and later proposals, the Government sought to have a key left on file by all users of cryptography, so that the Government would be able to read the full text of a message upon a proper showing of sufficient cause.[78] In response, supporters of strong cryptography claimed that the Government was exaggerating the threat posed by "the Four Horsemen of the Infocalypse"—terrorists, pedophiles, drug dealers, and money launderers.[79] The "Four Horsemen" term ironically lampoons the image of a future Internet dominated by numerous and dangerous criminals. As used by opponents of government surveillance, the "Four Horsemen" term invites us to consider whether law enforcement officials are overstating the criminal potential of the Internet while understating the usefulness of cryptography and of the Internet to a host of desirable activities.

The second wave of opposition to money laundering is just emerging. In December 1998 the Department of the Treasury proposed new "know your customer" regulations, using language that provoked a privacy alarm:

> As proposed, the regulation would require each bank to develop a program designed to determine the identity of its customers; determine its customers' sources of funds; determine the normal and expected transactions of its customers; monitor account activity for transactions that are inconsistent with those normal and expected transactions; and report any transactions of its customers that are determined to be suspicious, in accordance with the [agency's] existing suspicious activity reporting regulation.[80]

Concerning privacy, the proposed regulation has only a short and bland statement that does not address the range of privacy concerns expressed in this Article.[81] In immediate response to the proposal, press accounts appeared

---

78. *See generally* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Courts, and the Constitution*, 143 U. PENN. L. REV. 709 (1995).

79. *See, e.g.*, Keith Dawson, *Trolling Arms for a Horseman* (last modified Mar. 21, 1997) <http://www.tbtf.com/aresource/horseman-arms.html> (discussing Four Horsemen of the Infocalypse).

80. Know Your Customer Requirements, 63 Fed. Reg. 67,524 (1998) (to be codified at 12 C.F.R. pt. 21).

81.

> The proposed regulation requires banks to gather information about customers that, if misused, could result in an invasion of a customer's privacy. Accordingly, it is the [agency's] expectation

describing the rule as "an Orwellian intrusion into Americans' privacy."[82] Opposition arose from an "alliance of conservative, libertarian, and privacy groups."[83] (Less than three weeks after the regulation was proposed, the number of public comments to the FDIC topped 6,000, eclipsing the previous all-time record of fewer than 3,500.[84])

In considering the proposed expansion of money laundering laws, it is important to confront the extent to which such laws directly affect the sorts of privacy concerns explored in this Article. The proposed "Know Your Customer" rules vividly raise the question of the extent to which governments should enlist banks in the surveillance of private financial transactions. The proposed expansion of money laundering laws to cyberspace, along the lines contemplated by Welling and Rickman, could have an unprecedented effect of prohibiting cash transactions by ordinary individuals for ordinary purchases. The sharp political response to the "Know Your Customer" proposal suggests the unease felt in different parts of the political spectrum at the idea of the government requiring new levels of financial surveillance.

The next task is how to integrate law enforcement concerns with privacy concerns. This is no easy task. To begin with, law enforcement officials are emphatically correct that the "Four Horsemen" and other criminals might use the Internet in dangerous ways. For example, the insightful novel *Numbered Account*, by former Swiss banker Christopher Reich, tells a provocative story of how money laundering might be used to further both drug smuggling and international terrorist activities.[85] While recognizing the risks that the Internet can and will be used in some circumstances by criminals, I believe that the political debate to date has placed too much emphasis on the Four Horsemen

---

> that, in complying [sic] the Know Your Customer regulation, a bank will obtain only that information that is necessary to comply with the regulation and will limit the use of this information to complying with the regulation. Financial institutions need to safeguard and handle responsibly the information gathered in connection with complying with these obligations, and should integrate comprehensive privacy practices into their Know Your Customer programs.

Id. at 67,525.

82. Declan McCullagh, *Banking with Big Brother* (last modified Dec. 10, 1998) <http://www.wired.com/news/news/politics/story/16749.html>.

83. *Id*. Groups expressing opposition included the Free Congress Foundation, a conservative group, the American Civil Liberties Union, the quintessential libertarian organization, and the Electronic Privacy Information Center, often identified as a liberal, or at least proregulatory, group on many privacy issues. Strong opposition was also expressed by Republican Congressman Ron Paul of Texas, a member of the House Banking Committee. *Id*.

84. *See* Gabrielle Stevenson, *Record Response to "Know Your Customer": FDIC Receives More Than 6,000 Comments* (last modified Dec. 23, 1998) <http//www.worldnetdaily.com/bluesky_exnews/19981223_xex_record_respo.shtml>. The overwhelming majority of the public comments opposed the proposed regulation. *See id.*

85. CHRISTOPHER REICH, NUMBERED ACCOUNT (1998).

and other asserted risks.

Over time, perhaps, greater experience with the Internet will allow the political debate to take greater account of the following three points. First, evils such as drug smuggling, tax evasion, and terrorism have historically existed without the Internet. Cocaine and other illegal drug sales in the United States soared in the pre-Internet era. Second, whether the Internet increases or decreases the level of such evils is a complex empirical question, with no general answer. On the one hand, law enforcement fears that encryption will reduce detection of criminal activity. On the other hand, the Internet creates innumerable new flows of information, which may lead to a higher level of detection of criminal activity. Even if strong cryptography is available, criminals may not use it effectively or may have codes compromised (as in traditional law enforcement) by insiders who cooperate with the authorities. Criminals may also rely on the apparent security of cryptography to leave far more extensive records than would otherwise exist. If so, when such caches are revealed, then the net effect of cryptography may be to facilitate convictions.

Third, sustained and careful attention should be given to the benefits of cryptography and of other Internet activities and to the risks of new surveillance powers. Law enforcement officials, in light of their institutional responsibilities, have an obligation to explain the risks of criminal activity that can result from new technologies. The entire political process, however, should make the ultimate decision about how these risks of criminal behavior weigh against the benefits from the new technology and the risks created by new surveillance powers.

In the money laundering area, the argument for allowing anonymity and privacy is especially compelling for small denomination purchases that often reveal detailed and potentially embarrassing information about individuals.[86] The argument for government access to data becomes more compelling for large-denomination transactions, where concerns about money laundering and tax evasion are more salient. The technical problem at the core of the eventual financial privacy regime is whether we can create rules and institutions that approximate the status quo, with routine daily purchases often made in an untraced or secure way but with large transactions generally traceable. The key challenge for system designers, in a computerized setting, is to facilitate anonymous small transactions without creating a loophole that allows criminals or others to aggregate many anonymous small transactions

86. Welling and Rickman agree that policymakers should explore the possibility of creating a payment system where small-denomination purchases would not be traced on a mandatory basis. *See* Welling & Rickman, *supra* note 74, at 319.

into a large total. In electronic payments, as in realspace payments, some illicit transactions will occur. But mandatory government surveillance should only exist where its actual advantages outweigh the disadvantages.

D. Efficiency vs. Privacy?

In discussing the advantages of allowing flows of financial data to government, the focus has been on preventing or prosecuting illegal behavior. Greater information flows can restrict money laundering, help track deadbeat parents who fail to pay child support, and otherwise reduce the harms to society that inefficient surveillance permits. An even more general rationale, however, often exists for providing information to the government—efficiency. Free flows of information, in both the public and private sector, can lead to a variety of efficiency gains. Think, for example, of the burden of filling out government paperwork. Suppose that in an electronic future an individual would never have to provide information more than once to any government. In this technocratic utopia, the record would be entered once and then be available automatically for all authorized uses. With this efficiency in assembling and matching data, there would be far less burden on individuals who wish to apply for government benefits, enter into a contract with any government unit, file a report in connection with environmental or other regulatory programs, or otherwise transfer information to the government. Better coordination might also be possible between governments at the local, state, national, and even international levels.

In the private sector, free flows of financial data also create efficiency gains. From a seller's point of view, detailed information about the buyer allows more efficient provision of goods and services. Detailed information permits "one-to-one" marketing, so buyers get precisely what they most value, and so sellers can avoid unwanted inventory and can produce exactly what buyers want.[87] Ever-expanding computing power and the growth of the Internet mean that the costs of assembling, processing, and communicating personal data continue to fall rapidly. As the private sector develops new means for processing personal information, the information also becomes potentially available to the government.

---

87. On personalized marketing, see DON PEPPERS & MARTHA ROGERS, THE ONE TO ONE FUTURE: BUILDING RELATIONSHIPS ONE CUSTOMER AT A TIME (1993). For an analysis of the advantages and disadvantages of personalized marketing from a privacy point of view, see SWIRE & LITAN, *supra* note 1, at 142-44. In economic terms, detailed information about buyers can allow sellers to price discriminate more effectively, with efficiency gains resulting from the more precise matching of buyers' wants with sellers' products.

In the area of information processing, the public and private sectors are linked more closely than is often realized. Any data in private hands are only a subpoena away from the government. The efficiency gains in the private sector mean efficiency gains for law enforcement and the government more generally. The new flood of potentially available data, however, raises the possibility of disadvantages of government access to financial transactions. It is to these possible disadvantages that we now turn.

IV. DISADVANTAGES OF FLOWS OF FINANCIAL DATA TO GOVERNMENT

As the possible disadvantages of data flows are considered, it may help to imagine that the pipeline of data is going to three sorts of recipients: to the head of the FBI, such as J. Edgar Hoover; to every law enforcement official in the United States, as part of a database for investigating crimes; and to senior officials in a foreign dictatorship, who may use the data to enrich themselves and maintain themselves in power. One can hope and pray that worst-case scenarios do not occur. But contemplating the rogue government official, who might abuse private information, serves the same analytic purpose as contemplating the drug cartel or dangerous terrorist, whose bad acts might justify massive invasions of privacy. In both cases, examination of unusual scenarios clarifies the advantages or disadvantages of creating pipelines out of the vault. Once we understand the sorts of good and bad things that can result from data flows, we have a better understanding of what empirical questions to ask when designing or regulating a particular system of data flows.

A. Self-Interested Acts by Officials

Government officials might use the data to which they have access for personal financial gain, for political gain, or out of mere curiosity or prurience.

1. Financial Gain

Officials might gain financially from their access to other people's detailed financial records. First, the officials might use the data in their own business dealings. Access to detailed financial records might reveal confidential business information or otherwise give officials an advantage in choosing their own investments. Second, officials might get money from people who do not want their financial transactions revealed. When the

outside person approaches the official with an offer to pay hush money, the crime is called bribery.[88] An official might be bribed, for instance, not to collect all of the taxes legally due. When the official approaches the outside person for money, and threatens to reveal embarrassing or incriminating information, the crime is called extortion or blackmail.[89] A comprehensive database with every individuals' transactions might provide many opportunities for such blackmail. Third, officials might benefit financially by sharing the data with outside parties, who might pay an official for the data and then use the data for their own purposes. Sharing data with outside parties might also open up investments for officials that they could not otherwise afford. For instance, if confidential data revealed that a piece of expensive property would soon rise in value, then an official might join up with other "investors" to purchase the property.

In general, the greater the economic value of the data confided in officials, the greater the incentive for outside parties to corrupt those officials. A comprehensive database of transactions conducted by Americans would seem to be quite valuable, raising serious issues about how effectively such a database could be guarded over time. At a minimum, pipelines of information out of the vault and storage of data on the surface would have to be guarded carefully. For instance, good audit trails should exist for those who access the database, in an attempt to deter and detect illegal access to it.

2. Political Gain, Including Discrimination

Information is power, especially in the hands of powerful officials. The patterns of misuse for political gain track those for financial gain. First, the officials might use the data in their political dealings. The data may be an inexpensive and effective form of opposition research, and give officials inside information to make them more effective in achieving their political goals. Second, officials might use the inside information to extract concessions from the targets of surveillance, the way that J. Edgar Hoover apparently used secret files to protect his tenure in office and to influence policy debates. Third, officials might benefit politically by sharing the data with friendly outside parties. In wiretap scandals involving the Los Angeles police in the early 1980s, the police allegedly leaked confidential data to allies in right-wing political groups.[90]

---

88. *See* 18 U.S.C. § 201 (1994) (defining "bribery").

89. *See id*. § 1951 (defining "extortion" and related terms).

90. *See* Marc Cooper, *Wired* (last visited Jan. 20, 1999) <http://www.newtimesla.com/1998/081398/feature1-1.html>.

The possibility of leaks of this sort reminds us how personal data can be used to discriminate against individuals and groups. The most infamous example is likely the Nazi insistence in the 1930s that Jews give detailed reports of their financial assets. The Nazis then used these reports as part of a systematic program to seize Jewish assets.[91] More subtly, officials might use control over detailed financial information to favor or disfavor groups in the release of sensitive political data, the administration of regulatory programs, the award of government contracts, or otherwise. As Oscar H. Gandy, Jr. has explained, the "panoptic sort" of modern information systems "is a discriminatory technology that assigns people to groups of winners and losers on the basis of countless bits of personal information that have been collected, stored, processed, and shared through an intelligent network."[92]

3. Prurience

In addition to financial or political gain from the data, officials might snoop in personal financial records out of prurience or mere curiosity. There have been recurring revelations that IRS employees have gained unauthorized access to the tax returns of neighbors, celebrities, and others.[93] If officials also get complete access to the purchasing records of individuals, we might recognize the all-too-human temptation to see, for instance, precisely what was bought for a party in the home of a movie star or a prominent Senator. (And we might not be surprised if such details at least occasionally made their way into the supermarket tabloids.)

This sort of potential surveillance is chilling, in at least two respects. First, it sends a chill down the spine to think that their every move is subject to this sort of examination by unknown others. Life is less free and carefree when

---

91. For a discussion of this process of "Arisierung" (Aryanization), see ENCYCLOPEDIA OF THE HOLOCAUST 84-87 (Isreal Guttman ed., 1990); KARL A. SCHLEUNES, THE TWISTED ROAD TO AUSCHWITZ: NAZI POLICY TOWARD GERMAN JEWS 133-85 (1970).

92. Oscar H. Gandy, Jr., *It's Discrimination, Stupid!*, *in* RESISTING THE VIRTUAL LIFE 35, 36 (James Brook & Iain A. Boal eds., 1995).

93. One report found 1,515 "browsing" cases at the Internal Revenue Service in 1994 and 1995. Those whose files were accessed included Elizabeth Taylor, Dolly Parton, and President Clinton. One IRS employee was accused of spying on the records of Elvis Presley years after he died. Another IRS employee pled guilty to charges of looking up the salaries of a friend's coworkers to help the friend in a salary dispute at work. *See* Michael James, *Former IRS Clerk Pleads Guilty to Giving Friend Confidential Information*, BALTIMORE SUN, Dec. 3, 1998, at 2B.

In the wake of such revelations, Congress enacted legislation in 1997 to make browsing a felony. *See* 26 U.S.C.A. § 7213A (West Supp. 1998). The IRS has also instituted employee training programs. In 1994 the IRS disciplined 420 employees for browsing. This figure dropped to 371 in 1995 and 233 in 1996. *See* Rob Wells, *Congress Proposing Criminal Penalties on IRS Snoops*, ASSOCIATED PRESS, Apr. 7, 1997, *available in* 1997 WL 4860913.

one's every move is being tracked. Second, the surveillance may chill legitimate and desirable activity that would otherwise take place. For example, if financial records would reveal that a politician has seen a psychiatrist, and that revelation would be politically damaging, then the politician might not seek necessary medical help. As discussed above, courts in interpreting the First Amendment, have often struck down government controls over the flow of information as "chilling" of protected speech. Similarly, government insistence on tracking personal data can also chill legitimate activities of citizens.

B. Illegal but Non-Self-Interested Acts by Officials

The discussion of financial gain, political gain, and prurience assumed that officials were acting out of self-interest, pursuing their own interests rather than those of their principals, the government, and ultimately the people. Officials also might use financial data in the attempt to achieve what they believe to be good policy. An example might be an over-zealous prosecutor, who might use illegally-obtained financial information entirely in order to convict a criminal, with no thought of personal advancement.

An example of this sort of behavior recently surfaced in connection with hundreds of illegal "hand offs" of wiretapped phone conversations in Los Angeles.[94] Although there is no publicly available evidence that law enforcement officials used the information for personal gain, they did violate the rules restricting government surveillance. Those rules emanated from a constitutional or political judgment that the risks to privacy from certain types of surveillance outweighed the benefits of surveillance. When the government breaks its own privacy rules, there are privacy harms to all those, including the innocent, who were illegally put under surveillance. Citizens may lose trust in the government's general handling of personal information. More broadly, violation of the government's own rules cast doubt on the rule of law and the legitimacy of the government.

C. Access by Unauthorized Third Parties

In considering the disadvantages of access, the analysis thus far has focused on government officials who were authorized to see information but

94. "Hand offs" involve information from a wiretap of Person A illegally being used to start investigations about Person B, without revealing to B's defense counsel or anyone else that the tip originated from a wiretap. For financial information, analogous illegal snooping might reveal both petty and significant violations of tax and other laws. *See* Cooper, *supra* note 90.

used it in impermissible ways, such as for financial or political gain. As discussed in Part I, however, in connection with identity fraud, a major potential problem of government access to financial data is that the information may flow to unauthorized third parties ("UTPs").

In weighing the risks posed by UTPs, consider once again the difference between the impregnable vault 600 feet down and a flimsy shack housing data on the surface. Next think about the risks of disclosure when every law enforcement official in the United States has instant access to a category of information, such as arrest records, Currency Transaction Reports, or, in the future, the credit or debit card records of a criminal suspect. Among all the prosecutors, police officers, and clerks with access to such data, there will be some weak links or flimsy shacks. Some of them will seek personal or financial gain from their access to the data. UTPs will have many potential targets as they seek to find a "friendly" insider or a bribable one.

Even in the absence of a friendly insider, the government computer systems may not be secure. Skilled hackers may be able to tap the pipelines from the vault to the surface. Even more likely, they may be able to penetrate the defenses of the surface installation. The Defense Department reports hundreds of thousands of successful intrusions into military computers per year.[95] The actual damage caused by these intrusions is difficult to assess—many of the intrusions are undoubtedly done by teenagers and others who get access to part of a system but do not steal any sensitive data. The possibility of intrusions, nonetheless, is a powerful argument against allowing unlimited government access to sensitive personal information of any kind, including detailed financial information. If every law enforcement official in the country can access the data, then determined UTPs can, too.

D. Public Choice and "Mission Creep"

The uses and misuses of data evolve over time. The systems in place in one period can have a powerful effect on what systems will develop in subsequent periods. On the side of favoring government use of personal information, new uses of data may later become desirable once a system for collecting and disseminating the information is already in place. This argument is based on the idea of economies of scale. Once the costs of the database and infrastructure are already incurred for initial purposes, then additional uses may be cost-justified that would otherwise not have been.

---

95. *See, e.g.*, Tim Phillips, *Bits Krieg*, THE GUARDIAN (London), May 22, 1997, at 12 (quoting U.S. Defense Department official Robert Ayers as having said "I believe between a quarter and a half a million successful intrusions occurred in the US military computers in 1995.").

As an example, consider the argument that tax return information should be used by government agencies other than the Internal Revenue Service, in order to reduce the risk that well-off people will fraudulently receive government benefits. The economies of scale argument would point out that costs have already been incurred in the tax system to gather and organize the tax return data. Once those expenditures have already been made, there is a low incremental expense to transfer the data to other federal agencies and perhaps to state and local welfare and other agencies. An efficiency argument can then be made that additional uses of data, such as protecting against welfare fraud, should be authorized where the costs of gathering and organizing the comprehensive tax data would not have been justified solely to protect against welfare fraud.[96]

Although the economies of scale argument may be persuasive in some contexts, there are powerful counterarguments. For privacy advocates, the additional uses (and misuses) of data are examples of "mission creep," or a slippery slope down to a complete loss of privacy of highly personal information. Used in the context of the Vietnam War, mission creep refers to the risk that initial and justifiable government actions, such as collecting tax information or having a limited mission in South Vietnam, can evolve into unjustified and potentially tragic actions. If mission creep continues unchecked, tax returns might become essentially public documents. In recognition of this problem, there are federal laws restricting use of tax returns for other purposes.[97]

Privacy advocates have a large and probably often justified concern about mission creep. When the Social Security Number ("SSN") was introduced during the New Deal, for instance, promises were made that it would not be used as a national ID card.[98] Over time, however, SSNs have been used for an array of new uses. A proposed rule by the Department of Transportation, pursuant to a 1996 law, would take a major step toward using SSNs as national identity numbers. The proposed rule would mandate that state driver's licenses must contain SSNs to be acceptable for a range of

96. For a version of this argument, see Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 WM. & MARY BILL OF RTS. J. 455 (1995).

97. 26 U.S.C. § 6103 (1994).

98. In some settings, people "can be treated as criminals if they refuse to supply Social Security numbers, which President Franklin D. Roosevelt assured us would never be used for anything other than Social Security." Lisa S. Dean, *Q: Is a Nationwide Network for Immunization Records a Good Idea?; No: A Boon to Big Brother, This Effort Will Compromise Personal Liberty and Violate Privacy*, WASH. TIMES, July 27, 1998, Symposium, at 24; *see generally* ARTHUR ABRAHAM & DAVID L. KOPELMAN, FEDERAL SOCIAL SECURITY 141-143 (1998).

identification purposes, including boarding an airplane, being eligible for federal benefits, and purchasing a gun.[99]

The importance of the mission creep argument is heightened by an examination of the politics of privacy issues. In other countries, privacy laws have been decisively shaped by political mobilization against relatively simple and easily-understood threats to privacy. Prominent examples are the Australian defeat of a national ID card in the 1980s[100] and the German resistance to what were perceived as intrusive census questions in 1983 and 1987.[101] A 1996 law in the United States to create a national medical ID card similarly has met with significant opposition, and the Clinton Administration has stated that it will oppose implementation of such a card, until and unless broad new medical privacy legislation is enacted.[102]

In short, there is evidence that the political system may protect privacy relatively robustly when the issue is considered at the threshold, on the up-or-down question of whether an identification card should be created or some other surveillance project put into place. By contrast, a detailed and persuasive report on the American experience shows how difficult it has been for privacy advocates to succeed legislatively in the last two decades on less visible and more complicated privacy issues.[103] If the government (or private sector) already has fifteen uses for a category of data, it may be impossible politically to stop the sixteenth or seventeenth uses, even where those additional uses would never have been approved at the time the data collection system was first instituted.[104]

---

99. Jon E. Dougherty, *Controversy Swirls Around Repeal of National ID Law*, USA J. ONLINE, Aug. 5, 1998.

100. *See* SIMON DAVIES, BIG BROTHER: AUSTRALIA'S GROWING WEB OF SURVEILLANCE (1992).

101. *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 79-83 (1989). The political mobilization in connection with the German census was a key factor in the adoption of German data protection laws, which are among the most protective of privacy in the world. *See id*. at 82-83.

102. *See* Bill Nichols, *Gore Makes Protecting Consumer Privacy a Priority*, USA TODAY, July 31, 1998, at 6A (discussing Vice President Gore's speech announcing delay of national health identification program absent passage of new medical privacy laws).

103. *See* The Center for Public Integrity, *Nothing Sacred: The Politics of Privacy* (last modified July 28, 1998) <http://www.publicintegrity.org/nothing_sacred.html>.

104. The political analysis here is consistent with the predictions of public choice theory. In privacy debates, concentrated costs arise from restrictions on the government agencies or private-sector parties that wish to use the information. The benefits of privacy protection, by contrast, are diffused across the general population. For low-visibility and complex issues, the public is not likely to mobilize effectively to defeat the groups that would suffer concentrated costs from legislation. By contrast, the views of the general population are more likely to be effective politically for more easily-understood and salient privacy issues, such as the national ID card. For the public choice analysis, see Michael E. Levine & Jennifer L. Forrence, *Regulatory Capture, Public Interest, and the Public Agenda: Toward a Synthesis*, 6 J.L. ECON. & ORG. 167 (1990).

The historical examples of mission creep and the political history of privacy legislation return us to the "privacy paradox" discussed in the Introduction to this Article. The paradox suggested that, in the long term and taking a broad view, most people are concerned about invasions of privacy that might result from government access to sensitive financial and other records. But in the short term, when particular uses of data are at stake, the political system and many people prefer to let the information be used rather than to uphold privacy values.

The discussion here of the public choice of privacy legislation suggests important arguments for being cautious about expanding the government's access to personal information. Proposals for access should not be considered solely as a static matter, by evaluating only whether a particular pipeline is worth constructing. Instead, careful thought should also be given to a dynamic analysis of how data flows are likely to develop over time. Political mobilization on privacy seems more effective at the start, when a new mode of surveillance is being introduced, than in the detailed and technical debates that follow later.

E. Effects on Other Countries: The United States as a Beacon of Liberty?

The discussion thus far has focused on the effects within the United States of allowing or prohibiting pipelines of financial information to the government. This section considers how U.S. adoption of surveillance technologies may influence the surveillance technologies used in other countries, against both U.S. citizens and citizens of other countries.

It is possible, although not likely, that adoption of surveillance technologies within the United States will have positive effects in other countries. Supporters of traceable systems in the United States argue that such systems may help Colombia develop records about its drug cartels, perhaps eventually contributing to effective enforcement against the cartels. Similarly, traceable financial transactions might put pressure on criminals who take advantage of the banking and tax havens in the Caribbean and elsewhere. Transfers into the havens might become easier for authorities to detect, reducing the evasion of laws in the onshore countries. More generally, transactions by government officials would become more traceable, providing a possibility of accountability against corrupt officials. A future Ferdinand Marcos, for instance, might find it harder to hide large sums of money outside of the country.

On the other hand, it is far from clear that this gain in accountability would outweigh the ways that corrupt officials, in control of surveillance, could profit by using surveillance technologies against their citizens or ours.

It is possible that powerful new surveillance tools will be used to hold the powerful accountable. Study of the history of tyranny, however, suggests instead that powerful new tools will be used by the powerful and against the weak.

To assess the effects of U.S. adoption of surveillance technologies on other countries, consider both the technological and political reasons that U.S. policy may influence adoption in other countries. Consider, for instance, a U.S. law prohibiting anonymous electronic cash, or a U.S. banking policy that strongly encourages a fully traceable electronic payments system. As a technological matter, research and development in the United States is unlikely to focus on products that are illegal or discouraged in the United States. Similarly, research and development elsewhere in the world will be done with at least one eye on the U.S. market, the largest in the world. New technologies are thus likely to be consistent with the requirements of the U.S. market.[105]

The effect of U.S.-compliant technology on global payments systems is likely to be even greater for two other reasons. First, many international financial transactions originate, terminate, or pass through the domestic or international offices of U.S. financial institutions. These banks or other institutions are likely to have systems in place, even for their foreign offices, that are generally consistent with U.S. law. Second, the economics of computer systems, such as for a payments system, often seems to lead to dominance by one or a very few suppliers. For payments systems, there are probably important "network externalities," where the value of the payments hardware or software increases as others use the same system.[106] Automatic teller machine cards, credit cards, and debit cards all become more useful the

105. Even an apparent exception to the focus on the U.S. market turns out to reinforce the point. Strong cryptographic products (products that are difficult or impossible to decode) are an example, as of early 1999, where major research efforts are being undertaken outside of the United States.

A key reason why non-U.S. research is especially prominent for cryptography is that strong cryptography remains legal *within* the United States. United States restrictions today apply to *exports* of strong cryptography from the United States. A non-U.S. producer can thus sell cryptographic products world-wide, making it worth undertaking the research.

For most other actions subject to government surveillance, there is no similar advantage to having the product come from outside the United States. As emphasized in the text, if a payment mechanism or type of cellular phone cannot be used in the United States, then non-U.S. companies will likely choose U.S.-compliant technology rather than technology that is discouraged or illegal in the United States.

106. "Network externalities" exist where the value that purchasers place on a good increases as others buy the good. *See* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479 (1998). Such network effects are familiar from the fact that telephones, e-mail, and fax machines all become more useful as more people have compatible equipment.

more places accept a particular card. The same will be true of new Internet or other electronic payment systems. Where such network effects exist, the major international payments systems will almost certainly be usable in a major market such as the United States.[107]

The effects on other countries of U.S.-compliant technology are likely magnified by the effects of U.S. political actions. There are many subtle and not-so-subtle ways that the U.S. Government can encourage other countries to adopt measures that support surveillance. A notable example is the long-running diplomatic effort to convince other countries to implement anti-money laundering measures. Some countries, such as Switzerland, have recently and substantially expanded government access to previously-private financial information. In light of the unique role of the United States as a military, political, and financial superpower, other countries may find it easier to go along with U.S. surveillance initiatives than to risk a diplomatic fight.

Perhaps just as significantly, the U.S. decision to adopt surveillance technologies may make other countries more likely to use such technologies, even where the United States does not use diplomatic muscle on an issue. I call this the "Beacon of Liberty" argument, which has not been given the prominence it deserves in debates about surveillance. The "Beacon of Liberty" argument invokes the image of the Statue of Liberty in New York harbor. The upraised torch is a shining light unto the nations of the world, promising hope and liberty to all who see its beacon. With its Bill of Rights, its judicial and political protections against abuses of government power, and its civic tradition of individual freedom, the United States has a profound symbolic role, at home and abroad, as a guarantor of freedom.

Without seeking to romanticize history, the United States has often played an important role in seeking to promote freedom and democracy around the world. The United States has given a home to many immigrants and political refugees fleeing tyranny in their home countries. After World War II, the United States helped rebuild war-torn Japan and Western Europe into stable and prosperous democracies. Despite the strenuous objections of its British ally, the United States supported decolonization and the creation of democracies in the former colonies. During the Cold War, the United States used the rhetoric of freedom to oppose Communist countries that established secret police and pervasive surveillance over citizens' lives. More recently, the United States has supported democratization in countries all over the world. The list could go on.

---

107. *Id*. at 507-15 (discussing the network externalities of ATM and credit or debit cards).

With this legacy as a Beacon of Liberty, one might expect that the United States would use its moral authority to oppose the creation of government surveillance systems around the world. The United States might lead by example, permitting or encouraging technologies that promote privacy and individual freedom. The United States might encourage or require freedom-enhancing technologies, which would spread abroad. The United States might also employ its moral authority and diplomatic tools against surveillance. A model here could be the U.S. efforts to encourage human rights in other countries. For example, the United States can deliver foreign aid to countries only where the State Department finds a satisfactory human rights record.

Instead of applying its weight on the side of liberty, however, the United States is becoming a leader in requiring surveillance technologies. United States deployment of such technologies can embolden authoritarian regimes to deploy the same technologies and weaken U.S. complaints against authoritarianism. The moral authority of the United States will be on the side of government power rather than on the side of individual liberty.

For financial records, the clear example once again is U.S. insistence that strict money laundering laws be enforced at home and abroad. These laws provide governments easy and unprecedented access to information about many financial transactions. United States support for money laundering laws, moreover, makes it far more difficult to create anonymous payments systems over the Internet. As payments inevitably migrate over time to the Internet or other electronic means, individuals lose the ability to pay untraceably in cash. The requirements of money laundering laws, meant to stop a relatively small number of criminals, lead to the result that records of all electronic payments become available to the government.

The Beacon of Liberty argument is even more evident in the debate about "key escrow" proposals, such as those supported by the FBI. The FBI would like to receive the keys that would allow the government to open encrypted files. These keys would be available to the government on a real-time basis, so that the government could break into coded e-mail or hard drives without the knowledge of those writing or receiving the files. Key escrow, the current version of the "Clipper Chip" proposal,[108] has been enormously controversial, in part because it is designed to allow holders of the keys to read any message that falls into the key-holders' hands.

Key escrow is thus another example of U.S. leadership in seeking to

108. For a legal and factual discussion of the Clipper Chip, see Froomkin, *supra* note 78, at 709-897.

spread a surveillance technology to other countries. The U.S. Government has tried, with little success to date, to have other countries agree to a key escrow plan. One reason for the resistance is the reluctance of other countries to have the communications of their own citizens available to the U.S. Government. It remains quite possible, however, that law enforcement concerns will eventually be built into the infrastructure of encrypted files.

For both money laundering and key escrow, the United States is using its leadership on high technology and its diplomatic muscle to try to increase government surveillance of individuals. In addition, the harm to liberty in other countries may be more acute than in the United States itself. Other countries often do not offer legal protections to the individual that match those within the United States. In the United States, under current key escrow proposals, there would be a warrant requirement and other judicial oversight of investigations and prosecutions. Many countries give their officials greater access to data than is permitted in the United States. In some countries, there is a greater likelihood of corrupt officials, who will access the data themselves or make the data available to cronies. If we see the spread of key escrow and traceable financial transactions, as supported by the United States, then abuse of power by government officials will also spread, especially in the many countries that lack effective checks on government power.

In sum, there are strong technological and political reasons to expect U.S. adoption of surveillance technologies to influence other countries to adopt those technologies. As a logical matter, one might argue that the United States should use these technologies, because adequate protections exist in the United States to control abuse. The United States might then serve its historical role as a Beacon of Liberty to other countries, arguing against adoption of surveillance techniques in countries that do not enforce the rights of individuals. As a practical matter, and in order to avoid being labeled a hypocrite, U.S. adoption of surveillance tools will tend to increase use of the tools elsewhere, especially when the United States applies diplomatic pressure on other countries.

Within the broader inquiry of this Article, concerning the advantages and disadvantages of government access to data, the Beacon of Liberty argument suggests that U.S. adoption of surveillance tools can have significant negative effects elsewhere in the world. Those negative effects deserve careful consideration in U.S. deliberations about allowing pipelines of data to the U.S. Government. The concern is that the problems arising from traceability, which perhaps can be controlled within the United States, will turn out to be more pervasive in other countries. Instead of serving as a Beacon of Liberty, the United States instead might foster the creation of an

unprecedented system of global surveillance.

F. Distribution and Discrimination Issues

New surveillance technologies may have disproportionate impacts on different economic classes or racial or other groups. Earlier, in discussing self-interested acts of officials, the focus was on misuse of office to harm individuals or disfavored groups, such as occurred to Jews under the Nazi regime. The risk, in such circumstance, is that officials will use their access to financial data for their own economic and political gain, including the benefit of helping groups they favor and hurting groups they disfavor.

In addition to this sort of intentional discrimination, facially neutral uses of surveillance can have disparate impacts on racial or other groups. Professor Dorothy Roberts highlights this problem in her description of "welfare as a waiver of privacy."[109] Women welfare recipients, especially African-American women, have been the subject of detailed means and moral testing as a condition of receiving public assistance. Such testing "forces recipients to assume a submissive stance lest offended caseworkers cut them from the rolls. . . . Because families are not entitled to government support, the Supreme Court has reasoned, the government may force them to open up for inspection, shrink, rearrange, or break up in order to qualify for benefits."[110] Roberts concludes that welfare recipients are treated as "subjects" instead of "citizens": "While poor single mothers (subjects) must endure government surveillance for their paltry benefits, 'self-sufficient' traditional families (citizens) receive huge public subsidies—Social Security, tax breaks, and government-backed mortgages—without any loss of privacy."[111]

As government benefits shift from monthly checks to electronic benefits transfers ("EBT"), a new level of intrusion into the lives of those who receive welfare and other payments becomes possible. Previously, recipients could anonymously cash their checks or spend their food stamps. That is, the transaction did not link the individual to the purchase. With EBT, a permanent record of precisely what the person does with the government

---

109. Dorothy E. Roberts, *Welfare and the Problem of Black Citizenship*, 105 YALE L.J. 1563, 1579 (1996). Along with the sources cited in her discussion of privacy, Roberts reviews two books that document the intrusions into the privacy of welfare recipients, and especially African-American recipients, that welfare programs have historically permitted. *See* LINDA GORDON, PITIED BUT NOT ENTITLED: SINGLE MOTHERS AND THE HISTORY OF WELFARE 1890-1935 (1994); JILL QUADAGNO, THE COLOR OF WELFARE: HOW RACISM UNDERMINED THE WAR ON POVERTY (1994).

110. Roberts, *supra* note 109, at 1579-80 (footnote omitted).

111. *Id*. (footnote omitted).

benefit often will be created. This record system then has the potential to produce the full range of harms discussed in Part I: the harm itself (for example, a person inadvertently buys an ineligible product and thus loses food stamps); chilling effects (for example, eligible people refuse to accept benefits because of their fear of surveillance); cloaking effects (for example, elaborate barter arrangements emerge so that different purchasers can each buy the goods they want); and the burden of complying with surveillance (notably, negative feelings such as powerlessness from being subject to such surveillance).

Of course, some of these "harms" from surveillance are also advantages. Transactional records can reduce purchases of ineligible goods and purchases by ineligible recipients. That said, it should only take a small degree of empathy for most people to understand how burdensome it may feel to have one's every purchase potentially scrutinized by government officials, knowing that mistakes in purchasing could lead to loss of badly-needed income. As EBT programs are implemented, attention should be paid to the potentially large privacy implications. Good procedures should be created to limit officials' possible abuses of this new flow of information. For example, similar to tax returns, officials should not be permitted to browse in benefits records without a legitimate need to know. Where possible, an anonymity or cash-like option should be considered, so that poor people are not required to have their purchases tracked more than other people's purchases. Additionally, the agency should communicate the available privacy protections to recipients, so that recipients do not perceive risks of surveillance that do not actually exist.

The EBT discussion illustrates the disparate effects that can result from new surveillance technologies. Some surveillance systems, such as EBT for food stamps, apply predominantly to the poor and to minority groups that are disproportionately poor. The rich, the well-educated, and the savvy may also have ways, unavailable to the poor, to avoid or reduce government surveillance. Dummy corporations and off-shore accounts—prerequisites of the wealthy and sophisticated—can be effective in hiding one's financial transactions. Wealthy families today often help their children establish good credit histories, such as by paying off a credit card debt or helping with the down payment on a house.[112] In the future, these same families may train

112. Such efforts by the well-to-do can have important effects over time in the creditworthiness of their children and their consequent average level of financial success. *See* Peter P. Swire, *Equality of Opportunity and Investment in Creditworthiness*, 143 U. PENN. L. REV. 1533, 1542 (1995). In the future, a similar advantage may arise for the children of well-educated or wealthy families—that is, training in how to avoid leaving embarrassing records of purchases made in adolescence and

their children how not to leave a trail of embarrassing transaction records. As the next generation of surveillance systems develop, with their attendant risks for the individuals under surveillance, there will likely be disproportionate harms to certain groups resulting from such surveillance.

G. The First Amendment and Other Democratic Values

In presenting the anatomy of privacy harms, Part I discussed how First Amendment values are implicated by government and private-sector access to each book and web page that an individual has accessed. Such First Amendment concerns illustrate the way that highly traceable financial transactions can have important implications outside of the financial realm. By tracking the previously untraceable, financial records may reveal any number of things that were heretofore private. In considering the advantages or disadvantages of a pipeline out of the data vault, it is appropriate to think carefully about the range of effects of new uses of data.

In our most pessimistic moments, we might even contemplate how tracking of all financial transactions, perhaps combined with other forms of high-tech surveillance, might contribute to an increased risk of tyranny in a society. It is difficult to imagine how to study such an increased risk empirically; nonetheless, one source of freedom historically has been the necessary inefficiency of surveillance systems.[113] With better technology, society faces more explicit choices about whether categories of data will enter the vault and about what rules will govern access to the vault. If a society repeatedly opts for surveillance rather than privacy, then the nature of that society may change over time. That concern is an organizing theme of Alan Westin's classic book *Privacy and Freedom.*[114] As we look at vast new accumulations of financial records, or of other potentially revealing personal information, thought should be given to what other values, including the preservation of a free society, may in some way be at stake.

V. LESSONS FOR THE THEORY OF HIGH-TECH GOVERNMENT SURVEILLANCE

This concluding Part summarizes the analysis on government access to financial transaction records. It then shows how the same arguments can be

---

afterward.

113. My thanks to Larry Lessig for making the analogous point about how fair use in the intellectual property realm has historically been based on the inefficiency of the copyright monitoring systems available to copyright holders.

114. WESTIN, *supra* note 18.

used more generally to assess other forms of high-tech government surveillance and offers concluding thoughts.

A. Summary on Financial Transaction Records

The discussion to this point has focused on government having access to a certain sort of information—detailed records of what individuals have purchased. Part I showed reasons to believe that a much greater portion of financial transactions will be traceable over time. Part II introduced the metaphor of the vault 600 feet down. Once data is in the vault, legal and political decisions must be made about when and under what conditions to allow pipelines out of the vault. The anonymity option was also introduced because data can be filtered before it enters the vault.

Part III discussed the advantages of providing the government access to financial transaction records. The government has especially strong arguments for access with respect to its own financial transactions, such as tax receipts and grants of government benefits. The government can seek access for law enforcement purposes, to detect, deter, and punish illegality. More generally, the government (and the private sector) can make an efficiency argument that data be used where the marginal benefits of its use exceed the marginal costs.

In response, Part IV discussed the disadvantages of government access to this information. Officials might misuse the data, either for personal gain or out of an over-zealous desire to enforce the laws. Unauthorized third parties might misuse the data, for identity theft or other purposes. Public choice problems might lead to excessive access over time, as initially-justifiable uses of data become subject to overuse and mission creep. Decisions by the United States might have significant effects on data use in other countries, especially if the U.S. abandons its historical role as a beacon of liberty and instead encourages the use of surveillance technologies in other countries. Stepped-up surveillance can have troublesome distributional effects and result in racial or other discriminatory effects. Finally, the comprehensive tracking of financial records can implicate First Amendment and other values, potentially contributing in the long run to a less free society.

This list of potential harms in Part IV fleshes out the anatomy of privacy harms developed in Part I. For each the harms addressed in Part IV, the first and most obvious worry is the harm itself—from abuse of government office, identity theft, intrusion on First Amendment values, or whatever. Second, surveillance might lead to chilling effects, or actions foregone due to concerns about privacy. Third, surveillance might lead to cloaking costs, or actions taken to evade surveillance. Finally, there can be burdens of

complying with surveillance, from the time spent filling out mandatory questionnaires to the emotional strains that can result from being under observation.

B. Other High-Tech Government Surveillance

The advantages and disadvantages of government access are not limited to financial transaction records. The same structure of analysis applies to a broad sweep of other surveillance technologies that have been and will be developed. In the past, important databases developed in areas such as credit histories and lists of telephone calls made by each customer. In response, statutes were passed to regulate private- and public-sector access to those databases.[115]

Today we can perceive a three-step pattern for new systems of high-tech surveillance. First, new technologies make it potentially feasible and cost-effective to keep track of events or transactions—to put records into the vault 600 feet down. Second, records in the vault can be linked to individual names. Third, pipelines then can be readily created for letting information out of the vault, with persons on the surface using computer networks to search the vault by name or other criteria.

The use of closed-circuit television ("CCTV"), particularly in Britain, illustrates this three-step pattern. First, to an extent that would amaze most Americans, the United Kingdom has already placed CCTV cameras in almost all central cities as a device to combat crime.[116] The pictures taken by these cameras form the raw material to place in the vault. Second, face-recognition technology is now being tested that would allow CCTV pictures to be linked to individual names.[117] The third step, readily created once face-recognition technology becomes proficient, would be to have a searchable database of every person's movements as tracked by the ubiquitous CCTV cameras.

The routine tracking of peoples' movements may also be facilitated by the rapid spread of cellular telephones. Telephone companies today already keep

---

115. *See, e.g.*, Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681u (1994 & Supp. III 1997); Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522; Customer Proprietary Network Information Rules, 47 C.F.R. §§ 64.2001-64.2009 (1998) (FCC rules published pursuant to Telecomm Act of 1996).

116. *See* Steven J. Fay, *Tough on Crime, Tough on Civil Liberties: Some Negative Aspects of Britain's Wholesale Adoption of CCTV Surveillance During the 1990s*, 12 INT'L REV. L., COMPUTERS & TECH. 315 (1998); Nick Taylor, *Closed Circuit Television: The British Experience*, STAN. TECH. L. REV. (forthcoming 1999).

117. *See* Taylor, *supra* note 118.

records of the telephone numbers called by each customer. With cellular phones, however, companies gain the technical ability to track the location of the user of the cellular phone—how else can the phone company know which cell should receive the call?

From cellular phones, it may be only a modest step to wearable devices that handle other digital functions—access e-mail, keep a person's calendar, and generally provide all the convenience of a wearable computer. These devices could be physically trackable through the cellular phone technology just discussed. The convergence of phone with computers would also facilitate the automatic collection of many sorts of records. For example, it might become easy to discover that a particular phone call was made immediately after a particular e-mail was read. As voice-recognition technology becomes more useful, the built-in microphone might record some or all of what the user says during each day. More generally, the wearable computer-phone would offer incredible convenience to the user as a one-stop organizer of a person's digital life. It would also offer one-stop convenience for public- and private-sector actors who wished to keep track of that person's every digital move.

The examples of high-tech surveillance can be multiplied. E-mails are available to the government from the Internet Service Provider if it gets a proper subpoena. Web browsing records can become available as discussed in this Article. The transaction records kept by merchants and payment systems can be combined with demographic and psychographic data. And so on. As the costs of creating, storing, and distributing data continue to plummet, surveillance systems become feasible which would once have been unimaginable.

C. Conclusions

As frightening as these surveillance futures might be, so too are there wonderful benefits from the new technologies. The spread of the Web has helped many people realize the sweep of possibility that comes with instant and low-cost access to a worldwide network of (potentially) fascinating information. From an economic perspective, the stock market's enthusiasm for electronic commerce companies is based on a belief that individuals will choose to pay large sums of money in order to participate in new Internet activities. For those feeling overwhelmed by all of this information, the wearable computer offers the possibility of having a "digital secretary" that each person can train to select precisely the information that is of greatest interest. The science-fiction nightmares of surveillance are twinned with the science-fiction possibilities of a society brimming with new opportunities.

How then are we to think about the new information-collection systems, for financial records and more generally? This Article cannot offer a general answer, for all times and places, about when the government should have access to financial and other records. Instead, the Article systematically sets forth the chief advantages and disadvantages that should be considered for each surveillance technology. The chief advantages are efficiency and aid to law enforcement. The chief disadvantages vary with the circumstances but include the several arguments explained in Part IV. For CCTV, cellular phones, and wearable computers, one can consider the harms caused by privacy invasions, the chilling effects and cloaking costs, and the psychological and logistical burdens of living under a surveillance system.

In considering the new payment systems and other technologies, the principal legal and political questions will concern the use of anonymity (to filter data out before they reach the vault) and procedures (to regulate how data flow out of the vault to the surface). Concerning anonymity, government policy can require it, facilitate it, discourage it, or ban it. In this Article, during the discussion of money laundering in Part III, I recommended making strong efforts to facilitate anonymous payments over the Internet, at least for small transactions. This policy would uphold the status quo of having many ordinary purchases made by cash without leaving a permanent link to the individual. More generally, opportunities should be explored for allowing or fostering systems that do not automatically track data unless the benefits of such tracking clearly outweigh the disadvantages.

Concerning procedures, the American tradition of separation of powers offers a powerful tradition of having some independent judicial role when the government seeks access to private financial or other records. Special care is appropriate where the data concerns groups that may not be well-protected in the political system, such as recipients of electronic benefits transfers. For private-sector access to records in the vault, strong security measures are clearly desirable to prevent identity theft and other unauthorized use. Individuals likely deserve notice of how data will be used by those controlling access to the vault. Individuals also should have some ability to opt out of uses of data where it is reasonable to anticipate that a significant number of individuals would object to those uses.[118]

This Article began with the question of how you would like the government to have access to the records of every purchase you have ever made. In answering this question, there is no easy status quo on which we can rely. The old status quo for data privacy was relatively few databases and

118. For my views on private-sector uses of data, see SWIRE & LITAN, *supra* note 1, at 152-96.

few laws. Today the number of databases is growing rapidly, along with the links between them. If we retain a regime of few laws, then the government will be able to track us in many new and sometimes frightening ways. If we create a regime of many laws, then we risk cutting off valuable data flows in this information age.

Surely these are matters that deserve our careful and sustained attention.