PRIVATIZING INFORMATION AND INFORMATION TECHNOLOGY – WHOSE LIFE IS IT ANYWAY?

ELLEN DANNIN†

I. INTRODUCTION

On December 14, 2002, someone broke into the offices of TriWest Healthcare Alliance and stole all its computer hard drives containing information on 562,000 members of the military located in Arizona, Colorado, Idaho, Iowa, Kansas, Minnesota, Missouri, Montana, Nebraska, Nevada, New Mexico, North Dakota, South Dakota, Utah, Wyoming, and western Texas.[1] The information contained names, addresses, phone numbers, Social Security numbers, claims data, birth dates, duty stations, medical records, credit card numbers, and other information on active-duty military personnel and their dependents and retirees enrolled in TriCare through TriWest Healthcare Alliance Corporation, a managed care support contractor.[2]

It is possible the thief was simply looking for an easy target. TriWest's offices in Phoenix were so insecure that electronic door records show the thief made two trips into and out of the area.[3] The thief's identity remains unknown, in part because the office was not even protected by surveillance cameras.[4]

† Professor of Law, Wayne State University Law School. B.A. University of Michigan; J.D. University of Michigan. This paper was written with the assistance of a grant from the Economic Policy Institute. The author would like to thank Elliot Sclar for his suggestions.

1. David Pittman, *Suit Seeks Damages in Information Theft*, Tucson Citizen 2E (Jan. 31, 2003).

2. *Id.*; Dennis Wagner, *Lawsuit Accuses Triwest Healthcare of Negligence*, Arizona Republic 5B (Jan. 30, 2003); Josh Freed, *AP Newswire, Personal Data Of Military Members, Families Stolen: Computers Stolen From Triwest Office; Identity Theft Feared* (Dec. 26, 2002); Tom Philpott, *Military Update, Data Stolen On 550,000 TriCare Beneficiaries in 16 States* <http://www.fra.org/mil-up/milup-archive/12-25-02-milup.html> (accessed Sept. 30, 2003).

3. Philpott, *supra* n. 2.

4. *Id.*

But while it is natural to think of this only in terms of identity theft and the havoc this would cause those whose information has been stolen, it is possible the motives may have been more treacherous. It is likely that many of the military beneficiaries were preparing to be deployed to the Middle East in preparation for the war on Iraq. Someone who wanted to seek revenge on those involved and potentially weaken the resolve of the military in an invasion could use information to locate spouses and children and kidnap them or terrorize and then kill them.[5] So far nothing so terrible has happened. Indeed, some suggest that identity theft may be used in a more benign way simply to finance terrorism.[6]

Although the TriWest theft may be a worst-case scenario for contracting out information gathering and IT technology, it is not unique. Federal agencies planned to outsource thirty-three percent of their information technology projects in 2003.[7] Recently the federal government subcontracted the Defense Civilian Personnel Data System, which is essentially the human resources department for its civilian employees.[8] That subcontractor immediately re-subcontracted parts of the work to yet another firm.[9]

Again, what a treasure trove of information – home addresses and phone numbers, spouse's names, children's names, schools, and social security numbers, e-mail addresses, information about past employment and education, health records and disciplinary actions—whole lives and their intimate details laid out for the lucky person given access to it.

A terrorist or a criminal would rejoice in such great fortune. This information could be used for nefarious purposes such as identity theft – something that could net the perpetrator millions of dollars to fund the thief's projects. Even more worrisome is the possibility for blackmail to gain access to and control over employees in this critical department.

Maybe terrorists and criminals don't think this way. Or perhaps they do. If they do, the government needs to get serious about protecting the valuable, and potentially dangerous, information it

5. Wagner, *supra* n. 2, at 5B.

6. Joseph Farah, *WorldNetDaily: Homeland Insecurity: Are terrorists behind rise in identity theft? Computer-based crime wave sweeping U.S. could be major revenue source of enemy* <http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=30347> (Jan. 8, 2003).

7. Paul McDougall, *Outsourcing's On In a Big Way – CIOs See Promise and Problems in Increased Outsourcing*, Information Week G17 (Mar. 3, 2003).

8. PR Newswire, *Lockheed Martin Awarded $102 Million Contract to Support Defense Civilian Personnel Management Service* ¶ 1 (June 18, 2002).

9. *See* Blake Lewis, *Business Wire, ThinkSpark Signs $6.8 Million Agreement with Lockheed Martin for Department of Defense Civilian Personnel System* (July 16, 2002).

collects about each of us.

Once out of the government's sole control, opportunities for access multiply. Information can and does make its way around the world with the speed of light. U.S. companies use workers in countries such as India or Ireland to handle data because they speak English, are educated, and will work for a fraction of the salary of U.S. workers. But those cheap workers may come at a steep price. Every time information is transferred there is an opportunity to divert it. Given the nature of information in electronic form, these diversions may be hard to detect.

Despite what we have learned recently about how critical information technology is, how easily it can be misused, and how expensive that misuse can be, both federal and state governments are pursuing a course of privatizing information that seems to know no bounds. On July 21, 2004, Office of Management and Budget Deputy Director Clay Johnson identified information technology as a "real hotspot" for subcontracting when he spoke at a conference sponsored by the Contract Services Association of America. Of the $60 billion the White House has requested for IT hardware, software, and services in FY 2005. In FY 2004, the federal government spent $58.6 billion for private contractors to provide IT systems and services. Consulting firm Input predicts that figure will grow annually at a rate of 6.6% to $80.7 billion in FY 2009.[10]

The Reason Public Policy Institute (RPPI) reports that private companies now have contracts to provide a wide range of services that involve generating and collecting highly personal information.[11] These include social and mental health services; education, medication'* and psychiatric services; unemployment benefits processing; accounting and information technology; legal services; permit application, payment of taxes or fines, and car registration.[12] Add to these, contracts that relate more directly to IT services. Again, according to RPPI, the Treasury Department has contracted out its "information technology services, including networks, LANs, desktop computer setups, help desk support, and system administration."[13] Pennsylvania announced that it would consolidate and outsource all its agencies' data centers.[14] Connecticut

10. The Bureau of Natl. Affairs, *Outsourcing Opportunities Include IT, Training, and Property, OMB Official Says*, 42 Gov. Empl. Rel. Rep. 726 (Aug. 3, 2003).

11. *See* Reason Public Policy Institute, *Privatization 2001: E-government* 10 <http://www.
Rppi.org/apr2001.html/part2.pdf> (2001).

12. *Id.*

13. *Id.*

14. William Eggers & Adrian T. Moore, *The Heartland Institute, Privatizing the Information Highway* ¶ 2 <http://www.heartland.org/ia/febmar98/privatization.htm> (Feb. 1, 2001).

said it wanted to turn over all its IT functions to the private sector, because information technology was not seen as a core government function.[15]

In early 2003, the federal government announced plans to contract out the collection of back taxes.[16] In a 1996 test of private tax debt collection, contractors violated the Fair Debt Collection Practices Act and did not protect the security of sensitive taxpayer information.[17] In addition, a Treasury Inspector General for Tax Administration report expressed concerns with the IRS's contract administration and oversight of contractors based on

> reports and investigations of alleged criminal or civil misconduct in the procurement area in the last three years, including: contract workers at one lockbox bank losing or destroying more than 70,000 taxpayer remittances worth more than $1.2 billion; an IRS employee ensuring certain companies would receive contracts in exchange for illegal payments; and a contractor not being in compliance with the terms of its contract, which resulted in increased security risk at some IRS locations.[18]

A March 22, 2004 investigation found that an IRS "contractor's employees committed numerous security violations that placed IRS equipment and taxpayer data at risk. In some cases, contractors blatantly circumvented IRS policies and procedures even when security personnel identified inappropriate practices."[19]

This transfer of important functions from public to private control should be at the center of national debate. It affects our national security, our personal security, and our finances. Yet there has been

15. *Id*. at ¶¶ 4, 9. William Welsh, *Washington Technology, Connecticut's Rowland Pushes IT Modernization* <http://www.washingtontechnology.com/cgi-bin/udt/im.display.printable?client.id=wtdaily-test&story.id=16654> (June 6, 2001) (when Connecticut Governor Rowland was unable to contract out all IT functions).

15. The Bureau of Natl. Affairs, Inc., *IRS, NTEU Trade Arguments at House Hearing On Privatizing Collections of Overdue Taxes*, 41 Govt. Employee Rel. Rep. 549, ¶ 4 (May 27, 2003) (to allow the IRS to hire tax collectors) [hereinafter *IRS, NTEU Trade Agreeemnts*]. Alison Bennett, *House Approves Export Tax Measure Allowing Private Contractor Tax Collection,* 42 Govt. Empl. Rel. Rep. 597 (June 22, 2004).

16. *IRS, NTEU Trade Agreeemnts* at ¶ 11.

17. *Id*. at ¶ 14.

19. Treasury Inspector General for Tax Administration (TIGTA) TIGTA Audit Report #200320010 (Reference #2004-20-063), *Insufficient Contractor Oversight Put Data and Equipment at Risk* (Mar. 24, 2004) (cited in Greater Oversight Needed for IRA Contractors, TIGTA Says, 200 Tax Notes Today 143-69 (Jul. 26, 2004)). Contractor employees installed third-party email, Groupwise, chat, and instant messaging software on a third of the IRS computer workstations reviewed. These allowed them to send email outside the IRS offices and compromised security by potentially introducing viruses and spyware, bypassing firewalls, and allowing hackers who visit chatrooms to gain access to knowledge of the system's software architecture. *Id.*

deafening silence – except from privatization ideologues that cheerlead every movement from public to private control. But the time has come for national debate on this issue.[20]

II. CONTRACTING OUT INFORMATION GATHERING AND INFORMATION TECHNOLOGY

Go to http://www.maximus.com/public/virtual/government/child support. Click on the link, and you will be at the Nebraska Web page – http://www.nenewhire.com/. Assume you are an employer who by law must now report detailed information for every newly hired employee, including employee social security number, income withholding, and medical insurance verification.[21] Today, chances are you will meet this by filling out the form online through your state's Web page. Everything about the Web page will make it appear that you are dealing with the government, but, in fact, behind the scenes, you are probably providing this private information to a subcontractor.[22]

Or if you want to register your vehicle online in Arizona, you will actually be dealing with IBM, who "operates the program on its own servers, in exchange for one dollar per transaction and two percent of revenues."[23]

Or assume you are a parent with a child support order against you. Child support enforcement will locate the father, establish paternity, and collect child support.[24] But now the enforcers are likely to be private contractors, "bounty hunters" sent out to collect child support payments.[25] The private agency will be given access to personal information from government databases to be used in tracking you down and gaining compliance.[26] This may include drivers license data and tax return information, including social security numbers, home

19. *Id.*

21. *See e.g.* Robert Melia, *Pioneer Institute for Public Policy Research, Private Contracting in Human Services* ¶¶ 3, 7 <http://www.pioneerinstitute.org/research/whitepapers/wp03full.cfm>. Much of this reporting is driven by child support mandates. PSI, *Child Support, One Stop Reporting: Linking Employers to Child Support Customer Service* ¶ 1 <http://www.policy-studies.com/markets/ child_support/elink_sub.asp> (accessed Oct. 10, 2003).

22. PSI, *supra* n. 21; *Nebraska New Hire Reporting Directory* <http://Nenewhire.com/faqs/ index.html>.

23. Lisa Snell & Adrian Moore, *Intellectual Ammunition, E-Government* <http://www.heartland.org/ia/novdec99/privatization.htm> (Nov. 1, 1999).

24. *See e.g.* Melia, *supra* n. 21.

25. U.S. Gen. Acctg. Off., *Child Support Enforcement: States' Experience with Private Agencies' Collection of Support Payments*, GAO/HEHS-97-11 at 2 (Oct. 1996); *see e.g.* Policy Studies Assoc., Inc. <http://www.policy-studies.com/privatization/priv_full.htm>.

26. *Id.*

addresses, sources of earned income, including employer address, and sources of unearned income, such as bank accounts or mutual funds.[27] Nebraska and Tennessee have given contractors even greater access to tax information than the IRS permitted under laws intended to protect confidential information.[28] Once a support order exists, the agency monitors, records, and distributes payments and can enforce delinquent payments through an array of collection methods.[29]

Opponents of what they call "bounty hunter" proposals object to making such a wide range of information available to private collection agencies that can contract with custodial parents to collect unpaid child support.[30] The Center for Law and Social Policy (CLASP) argues that federal and state databases that some want to make available include "confidential financial, employment, and medical insurance data obtained from the Internal Revenue Service, financial institutions, employers, interstate law enforcement networks, corrections systems, unemployment compensation programs, and many other public and private data sources."[31]

The Privacy Rights Clearinghouse notes: "Virtually every major change in life is recorded somewhere in a government document. Shortly after you are born, a birth certificate is issued; if you obtain a driver's license, get married, buy a house, file a lawsuit – all of these events are recorded in public documents easily available to you and to others."[32]

---

27. U.S. Gen. Acctg. Off., *Child Support Enforcement: Early Results on Comparability of Privatized & Pub. Offs.*, GAO/HEHS-97-4 at 14, 27 (Dec. 1996); *see e.g. Maximus, Helping Government Serve the People, Project Map* <http://www.cortidesignhost.com/maximus/ childsupport/projmap.html> (accessed Oct. 22, 2003) (listing the states with current Maximus child support offices).

28. U.S. Gen. Acctg. Off., *supra* n. 26, at 15. The report provides details of various parties' positions as to disclosure and the impact of current and then contemplated law on its disclosure. *Id*. at 15-16. The IRS' denial of access to certain information does not mean that it has not been made available from other entities that collect similar information. *Id*. at 14-16, 35.

29. *Id*. at 27.

30. Vicki Turetsky, *Congress Should Reject "Bounty Hunter" Proposals to Open Child Support Data Bases and Enforcement Tools to Commercial Agencies* ¶ 3 <http://www.clasp.org/DMS/ Documents/998764702.465/doc_Senfact.PDF> (accessed Oct. 1, 2003).

31. *Id.*; *see also AFSCME Leader, Privatization Threat Thwarted on Capitol Hill* <http://www.
afscme.org/publications/leader/2000/00090108.htm> (Oct. 2001). The Internal Revenue Service itself proposes using private collection agencies to track down debtors despite concerns of increased cost from using private contractors and privacy concerns. *See* The Bureau of Natl. Affairs, Inc., *supra* n. 16.

32. *From Cradle to Grave: Government Records and Your Privacy* ¶ 2 <http://www.Privacyrights.org/fs/fs11-pub.htm> (accessed Sept. 23, 2003).

The range of private involvement with information collection, acquisition, and retention is breathtaking. It reaches into every area of government and the lives of the public. As more government services are delivered through online transactions, more of them will be provided to some degree by private contractors.[33] For example, in 2000, Lockheed Martin won a $102 million contract to control human resources for civilians working for the military, the Defense Civilian Personnel Data System.[34] Lockheed Martin, in turn, subcontracted part of the work to ThinkSpark.[35] SDR Technologies develops software for the government and runs it on its own servers at no charge to the agency. It is compensated on a per transaction basis.[36] A contractor hired by the IRS to develop software was found to have a pattern of violations of IRS security policies, yet IRS management gave the same contractor root access for fifty of its employees to the IRS' operating environment for the same system. The IRS granted the request because otherwise it was unable to ensure the network was properly configured.[37] "Root-level access [to] a computer system allows the user to make unlimited and unrestricted changes to any part of the computer system, including the operating system and any applicable computer applications. In many cases, a user with root-level access could turn the audit trail off and/or erase audit trail data, without any record as to who used the root-level privilege."[38] In 1997, Pennsylvania announced that it would consolidate and outsource all its agencies' data centers.[39] The Reason Public Policy Institute report on privatization during 2000 provides examples of the wide range of information collection and data

33. Snell, *supra* n. 23, at ¶ 1; Jerry Mechling & Victoria Sweeney, *Finding and Funding IT Projects, Part 3: Performance Contracting* ¶1 <http://www.govtech.net/publications/gt/1998/ mar/financing/financing.phtml> (accessed Sept. 23, 2003).

34. PR Newswire, *Lockheed Martin Awarded $102 Million Contract to Support Defense Civilian Personnel Management Service* ¶ 1 (June 18, 2002); Reason Public Policy Institute, *Privatization 2001: Public-sector Trends* ¶1 <http://www.rppi.org/apr2001.html> (2001).

35. *See* Lewis, *supra* n. 9; *see also* Army Civilian Personnel Online, *Modernization* <http://www.cpol.army.mil/library/modern.html> (last accessed Oct. 13, 2003).

36. Snell, *supra* n. 23, at ¶ 10.

37. Treasury Inspector General for Tax Administration (TIGTA) TIGTA Audit Report #200320010 (Reference #2004-20-063), *Insufficient Contractor Oversight Put Data and Equipment at Risk* (Mar. 24, 2004) (cited in Greater Oversight Needed for IRA Contractors, TIGTA Says, 200 Tax Notes Today 143-69 (Jul. 26, 2004)). This meant that the contractor or a hacker could navigate the system and gain access to taxpayer information. *Id.*

38. *Id.* at n. 1.

39. Eggers, *supra* n. 14.

retention that are involved in subcontracting,[40] including social and mental health services, such as education, medication and psychiatric services;[41] processing of unemployment benefits;[42] accounting and information technology;[43] legal services;[44] permit application, payment of taxes or fines, and car registration.[45]

Rather than considering whether this massive move from public to private control is wise, the government sees its information technology systems as especially appropriate for privatization.[46] Why? One reason is that government has failed to develop sufficient in-house expertise. As a result, government now has no choice but to turn to private companies for expertise in this rapidly developing area. In addition, equipment and software costs are high,[47] and keeping up with constant change in technology has been seen as too difficult.

A second reason is that some in government believe it should "divest" itself of those functions that are not seen as core government functions, a management philosophy recently popular in the private sector. Information is a function that can be categorized as a non-core function, and thus one to be contracted out. In 1999, Connecticut, for example, announced it wanted to turn over all its IT functions to the private sector because information technology was not seen as a core government function.[48] In the end, it chose not to do so, but many other states and local governments have.[49]

Well, so what if what once was government information is being

40. *See* Reason Public Policy Institute, *supra* n. 11.

41. Reason Public Policy Institute, *Privatization 2001: Public-sector Trends* 5 <http://www.rppi.org/apr2001.html/part1.pdf> (2001); Reason Public Policy Institute, *supra* n. 11, at 11.

42. Reason Public Policy Institute, *Public-sector*, *supra* n. 41, at 5.

43. *Id.* at 5, 7.

44. *Id.* at 5-7.

45. Reason Public Policy Institute, *E-Government*, *supra* n. 11, at 8, 11.

46. Darrell A. Fruth, *Note: Economic and Institutional Constraints on the Privatization of Government Information Technology Services*, 13 Harv. J.L. & Tech. 521, 521-22 (2000); Eggers, *supra* n. 14, at ¶ 1. The National Center for Policy Analysis suggests that "ATM-like kiosks" could be used to let people use their credit cards to pay parking tickets, get information on property taxes, or prepare divorce papers. *Natl. Ctr. for Policy & Analysis, Govt. & Pol., Automated Kiosks for Divorces, Fines & Taxes* ¶1 <http://www.ncpa.org/pd/govern/oct97a1.html> (accessed Sept. 23, 2003).

47. Mechling, *supra* n. 33, at ¶ 2.

48. Eggers, *supra* n. 14, at ¶¶ 4, 9; *see* Fruth, *supra* n. 46, at 529.

49. Edward McKenna, *Washington Technology, Outsourcing Efforts Gather Steam Among Federal Agencies: States Towns Progress Despite One Dead* ¶¶ 1-4 <http://www.washingtontechnology.com/news/14_24/tech_features/1153-1.html> (Mar. 20, 2000). The governor then privatized parts of the state's IT system. William Welsh, *Washington Technology, Connecticut's Rowland Pushes IT Modernization* ¶¶ 1, 3-4 <http://www.washingtontechnology.com/news/16_5/state/16643-1.html> (June 4, 2001).

subcontracted? Does it matter where this function is lodged in the private or public sector?[50] So far cheerleading for privatization has been all that has been heard. But there are potentially disastrous consequences for national security, personal security, and economic security if this unasked, unexplored question is answered wrong.

Furthermore, the dimensions of the problem and the importance of getting it right increase every day. As governments increasingly employ information technology, they are doing more than just providing traditional services more quickly and at lower cost. They are also restructuring the form of government.[51] This restructuring has many positive aspects, for example, making it possible to check for information or perform other transactions online rather than in line. But, on the other hand, those who lack easy access to computers will be increasingly marginalized and shut out from their government. In addition, if the entity performing these information services is not really the government, they are at an ever-greater remove and probably have less access and ability to call the government to account.[52]

Answering the question whether it makes a difference that the entity with access to and control of information is private rather than public ultimately requires considering whether government differs from private. Fortunately, while we as a nation must confront that question at some point, we can assess many key issues about privatizing public information collection and retention in the absence of an answer to issues of accountability and governance.

As a first step, we need to ask: What is special about information, if anything? The second question, also ripe for exploration, is whether information in private rather than public hands is likely to create special problems. This then leads to the third question: whether there are ways to prevent or remedy any problems that arise.

A. IS INFORMATION SPECIAL?

In a sense, information is simply a form of property. Private subcontractors are often given, leased, lent, or sold government property to allow them to perform the job. These can include buildings, vehicles, or other specialized equipment, or they may acquire property while performing the job. Examples may be revenue generated, such as parking fees collected; property built or acquired, such as buses or

50 For a discussion of this question in terms of accountability, *see* Ellen Dannin, *Privatization, Accountability, and Public Welfare*, Annual Meeting of the Law and Society Association, Chicago, Illinois (May 27, 2004).

51. Fruth, *supra* n. 46, at 522-24.

52 Ellen Dannin, *One Person's Red Tape is Another's Accountability: Privatization, Accountability, and Public Values* (July 23, 2004) (unpublished manuscript, on file with author).

buildings; or improvements.[53] Public information can also be given to a contractor to enable it to do a job, or it can be acquired as the job is performed, or acquiring information may be the object of the contract.

But it is just as plain that information is more than simply another form of property. Information has unique qualities that make it especially valuable and highly marketable. Whereas a bus has a limited number of uses, most of which are easily foreseen, the uses of information are only limited by the imagination of the one with access to, or possession of, the information. Perhaps most important, and unlike physical property, information is almost infinitely replicable. It can be returned to the government at the end of a contract and sold on the market and also retained by the subcontractor. Information is thus more like a life form than real property. With information now in electronic form, this quality has been enhanced.

Access to and use of information is highly dependent on the medium within which it exists. Thus, when a contractor contracts for the use of its computer equipment to perform a job, especially when it designs – and owns – the software, it is in a unique and powerful position with regard to access to the uses of that property and the information retained on the hard drive.[54] As a result, a government agency may find that, even if it is dissatisfied with the contractor's performance and has the right to terminate the contract, termination will be so costly that it is virtually impossible to do so. There will be a large sunk cost in the development of the software, and the government may not want to face having to develop new software if it moves to a new vendor.

The software itself may affect whether and how the data can be retrieved or used with other software. Assuming the data can be exported from its software environment, it might still be necessary to re-enter all the data. It can be very expensive and disruptive to terminate this sort of contract. There will be costs to retrain employees who work with the data and lost time and efficiency during the training period and changeover. Depending on the contract's language, the contractor might claim that it owns the data, not the government. In short, the government agency that enters into these contracts may lack effective means to discipline the contractor and enforce its rights. And if the government cannot do these things, it cannot protect the public's interests, including the public's information.

According to RPPI, the Treasury Department contracted out its

53. *See* Ellen Dannin, *To Market, To Market: Caveat Emptor*, *in* To Market, to Market: Reinventing Indianapolis 22-26 (Sheila S. Kennedy & Ingrid Ritchie, eds. 2001).

54. *Cf.* Reason Public Policy Institute *Privatization 2001: E-Government* 10 <http://www.rppi.org/apr2001.html> (2001).

"information technology services, including networks, LANs, desktop computer setups, help desk support, and system administration."[55] One wonders exactly how much thought the government gave to the consequences of this degree of outside control over and access to valuable private information. Did they consider only the cost of the contract and whether it was cheaper? Did they enumerate and then cost out the consequences of failure by the vendor? Certainly, if problems arise, there may be a high price to pay for what seem to be lower-cost IT services.

We already have stories of unforseen negative consequences from moving valuable information from public to private control. The story of what happened to the *Journal of the National Cancer Institute* provides an example of what can be lost when information paid for at government expense moves from public to private hands.[56] Originally, the *Journal* was printed through the Government Printing Office.[57] By 1992, the semimonthly Journal was selling 6,240 copies at an annual subscription of fifty-one dollars, was distributed free to more than 800 depository libraries, and was recognized for publishing the best original research papers in oncology from around the world.[58] In 1993, the National Cancer Institute instituted a program that made access to the *Journal* twice as expensive.[59] For this, the International Cancer Information Center, publisher of the *Journal*, received a Federal "Hammer" award.[60] In January 1997, it was privatized.[61] Ownership was transferred from the National Cancer Institute to Oxford University Press.[62] No free copies would be provided to Depository Libraries, and subscription prices rose to $120 for an individual and $150 for an institution.[63]

The result is a tightening up of the flow of scientific information. The change made it more expensive and difficult to disseminate information that can make a difference in life or death. It also means that a resource and infrastructure developed with extensive public

55. *Id.*

56. Wayne Kelly, Speech, *Privatization of Federal Government Information* (Federal Documents Task Force Midwinter meeting, Feb. 15, 1997) in Issue 12/13 Progressive Librarian, ¶ 7 <http://www.libr.org/PL/12-13_Kelly.html> (Spring/Summer 1997).

57. *Id.* at ¶ 3.

58. *Id.* at ¶ 4.

59. *Id.* at ¶ 5.

60. *Id.*

61. Wayne Kelly, Speech, *Privatization of Federal Government Information* (Federal Documents Task Force Midwinter meeting, Feb. 15, 1997) in Issue 12/13 Progressive Librarian, ¶¶ 6, 7 <http://www.libr.org/PL/12-13_Kelly.html> (Spring/Summer 1997).

62. *Id.* at ¶ 6.

63. *Id.* at ¶ 7.

funding now exists to enrich an institution and not to benefit the public. Wayne Kelly, the Superintendent of Documents for the Government Printing Office raised additional important questions about the change:

> Looking through the *Journal*, a number of questions come to mind. I note that the masthead lists some 26 staff members. I wonder if the editorial and news staff is still being paid by the American taxpayer, but working for the Oxford University Press? I wonder if the Oxford Press is sharing revenues from the new, higher subscription rate with the National Cancer Institute? I wonder if copyright will prevent a librarian from sending a copy of an article to another librarian? I have no way of knowing the answers to these questions, because the details of the Cooperative Research and Development Agreement are not public information, according to NCI legal counsel.[64]

In recounting this story, Wayne Kelly asked questions in 1997 that have yet to enter the public debate. Perhaps, with stories about sales of private financial information, Ptech and its potential links to terrorism,[65] and continuing corporate scandals, we are at last ready to take a look at them:

> But what if this new trend drives future Federal Government Information Policy? Since the founding of our nation, the cornerstone of information policy in the United States has been the principle of universal access to Federal information. This principle is being set aside without many of the usual checks and balances in our democratic society: Without any high level policy debate, without clear rules, without thought to unintended consequences, and often without full public disclosure of the negotiations and agreements.
>
> Is all Federal information with sufficient demand going to be sent to market? If so, we should think about what that means.
>
> Does it mean that a Government agency may sell its name as well as its information?
>
> Does it mean that a wide array of private sector publishers will no longer have access to the information to add value and redistribute it to many different markets in different products?
>
> Does it mean the public consumer must pay two or three times as much, or more, for the same information?
>
> Does it mean that agency publishers will focus their attention on more popular, marketable information and eliminate other, perhaps more significant but less marketable information?

64. *Id.* at ¶¶ 11-12.

65. McDougall, *supra* n. 7, at ¶ 22.

> Does it mean that programs authorized by Congress will begin to move away from public needs, to focus instead on market needs never contemplated by our elected representatives?
>
> Does it mean Government employees working at taxpayer expense to support the information requirements of private firms? And isn't that corporate welfare?
>
> And what if the *Journal of the National Cancer Institute*, now owned by the Oxford University Press, does not meet the profit goals of the new owner? Does it mean that instead of a "Hammer" award, there will be the "axe" usually awarded sub-par performers in the market place?
>
> Who represents the public in a Bottom-line Information Era?
>
> What is to prevent our nation's bridge to the 21st Century from turning into a toll bridge for Government information?[66]

Even more stories can be added. There was the West Publishing case. West publishes a wide range of legal materials, including volumes of legal cases and statutes for nearly every jurisdiction in the United States. At one point, West claimed it owned the governmental materials it had published, not just copyright in the format in which it presented them.[67] These cases and statutes were provided to West – and to any other publisher – free and at taxpayer expense. Eventually a legal case resolved the issue of ownership.[68] But lawsuits are costly even for the winner. Who will be the next entrepreneur who attempts what West did – ownership in the public's information? Ownership means the right to exclude others and the right to profit from specific property. We have seen a debate about claimed ownership in genetic information. We may yet see the day when someone claims ownership in our personal information just because it was in a government database transferred to a private contractor.[69]

As mentioned before, information differs from other forms of property in that it is more like a life form, because it can replicate, or at least it can be copied. Once this meant scribes, then typists, and later

66. Kelly, *supra* n. 56, at ¶¶ 15-25.

67. Gary Wolf, *Who Owns the Law*, Wired ¶ 3 <http://www.wired.com/wired/archive/2.05/ the.law.html> (May 1994) (however West lost the case); David Cay Johnston, *West Publishing Loses a Decision on Copyright*, N.Y. Times D 1 (May 21, 1997). Communications Media Center at New York Law School, *West Publishing Loses Decision on Copyright* <http://www.cmcnyls.edu/Bulletins/ WLLCRDC.htm> (May 22, 1997).

68. Johnston, *supra* n. 67, at ¶ 3.

69. Kelly, *supra* n. 56, at ¶ 3.

photocopying. Now information is in forms that mean an infinite number of originals can be created in seconds. A private contractor at the end of its contract term could potentially return all data in its possession to the government while also secretly retaining the same data. A contractor could release or sell or distort data in ways not previously possible. You cannot do this sort of thing with busses or fees paid for access to national parks. To provide the assurance that none of this information has been retained will require technological solutions beyond mere inventories or balance sheets.

Few realize that as many government functions are contracted out as are contracted back in. As more information and IT services are contracted out,[70] there will be more and more information that we cannot be certain has left the hands of those no longer legally entitled to possess it.

Again, although a form of property, information is special. The damage that can be done by a private contractor in possession of a bus owned by the public is limited. But misused information has enormous potential to harm people and government. Clients of public mental health services would want information they provide to remain confidential.[71] The same is probably true of those who seek HIV testing, regardless of the test results. Although not necessarily confidential, information acquired while performing public agency accounting functions is also likely to generate valuable information needing careful handling.[72] Add to this the release of personal information (home address, dependents, or benefits usage) connected with those providing national security. The potential for harm is enormous

In sum, then, while information may be regarded as just another function – and not a core one at that – or as just a form of property, this is far too cavalier a way to treat it. It combines the qualities of being highly valuable, potentially damaging if released, easily replicable, and being difficult to trace if wrongly released. Add to that the fact that the current administration and state governments are bent on privatizing IT and so far have proven to be unconcerned about our welfare.

70. Mildred Warner & Amir Hefetz, *Privatization and the Market Role of Local Government: Small Growth in Contracting Underscores Dominance of Service Provision by Public Employees*, Economic Policy Institute Briefing Paper 15 <http://www.epinet.org/content.cfm/ briefingpapers_bp112> (accessed Oct. 13, 2003).

71. *See* Reason Public Policy Institute, *Privatization 2001: Public-sector Trends* 5 <http://www.rppi.org/apr2001.html> (2001).

72. *See id.*

B. ARE THERE SPECIAL PROBLEMS THAT MIGHT ARISE CONCERNING SUBCONTRACTED INFORMATION?

Contractors who have access to or store confidential information do realize that they need to give confidential information a high degree of security.[73] We can assume that most will perform their jobs ethically and as intended. But in order to avert problems and plan defenses, you have to look at worst case scenarios – not the good guys. Or at least remember that those we once thought were the good guys now have officers doing "perp walks." Given the importance of information and the enormous harm that can flow from its misuse, it amounts to criminal misfeasance to assume the best, even though the best may occur most of the time. Are there plausible scenarios that might lead to a misuse of information?

You would have had to have been totally isolated from the news the past three years not to come up with highly likely scenarios. We can conclude that terrorist attacks, fears of such attacks, financial wrongdoing, sales of personal financial data will happen, because we know they have happened. While future events may not be exact repetitions, this recent past points out the paths we need to be looking along.

Financial exigency is certainly likely to press a contractor – or a contractor's employees – to misuse information. We are in the midst of economic downturn, and there is a lot of financial exigency going around. A contractor that finds itself in financial straits or even a contractor with a low level of ethics and a strong desire to maximize its profit may find it difficult to forgo the temptation to make use of the valuable commodity that private information is. In 1987, Ronald Moe observed: "The stakes for private parties are often high, and they may be willing to go to the edge of the law. Thus the potential for corruption during the contract stage of the delivery process is considerable."[74] Recent case studies published by Ingrid Ritchie and Sheila Suess Kennedy in *To Market, To Market: Reinventing Indianapolis*[75] demonstrate just how common corruption can be, especially when an administration is blinded by pro-privatization ideology – and just how greatly this can harm the public welfare.

Recent experience with the unethical or even illegal lengths to which even large companies will go to generate profits, coupled with the problems many have experienced with identity theft, suggest that

73. *See generally* Policy Studies Associates, Inc. <http://www.policystudies.com> (accessed July 7, 2004).

74. Ronald C. Moe, *Exploring the Limits of Privatization,* 47 Pub. Admin. Rev. 453, 458 (1987).

75. *See generally To Market, To Market: Reinventing Indianapolis*, *supra* n. 53.

problems in this area are likely. Information provided with no more protection than a mere agreement or hope that the contractor keep it confidential creates a dangerous situation. While information can be transferred or shared these days with great ease, it is devilishly difficult to monitor and prevent its wrongful dissemination and then to remedy its misuse.[76] Consider Nebraska's Web page for employer reporting on new hires. An employer might not realize it was providing information to Maximus (although this information is available if the correct link is clicked). The employee whose information has been provided – but who will be unaware of the medium used to provide it – is the one likely to suffer harm and is particularly vulnerable. The employee might realize her private information has gotten into the hands of wrongdoers when the credit card bills arrive, but is unlikely to be able to trace how that private information was released and seek recourse.

Is government any better at keeping secrets? We can all think of leaked information. We all know that some government employees have been corrupt, but the very nature of government as a non-market institution means that it does not face the same financial pressures as private entities. Simply put, government agencies have less incentive to behave opportunistically in the ways that might lead to the misuse of private information.[77] Privatization proponents argue that market forces resulting from competition promote lower cost and higher quality than is possible in the public sector, which is shielded from the market. If the market and competition are that powerful in promoting positive ends, we need to remember experiences that demonstrate that market forces can also lead to deception and corruption and enormous harm.

In other words, when the information under consideration has a market value it may need to be protected from the consequences of market forces. This suggests that in making the decision whether to contract out, the government ought to consider whether this is a situation in which it ought to opt for stability and lack of market competition. If this is the case then contracting out is not appropriate. We also have to be concerned about the national security value of some information. Such information would attract buyers who have shown they have very deep pockets. Again, the harm suffered does not warrant even large savings.

What is particularly worrying is that the government has crippled itself so that it now lacks the ability to protect us. If it is true that private contractors have greater incentives to misuse information, then government must exercise even greater oversight over private

76. Turetsky *supra* n. 30.

77. *Cf.* Fruth, *supra* n. 46, at 533.

contractors.[78] This will increase the costs of contracting out. But if a reason for contracting out information services is that government lacks expertise, then how is government to exercise any effective oversight?

C. THINKING ABOUT WAYS TO PROTECT INFORMATION FROM ABUSE

Obviously, the executive branch should be thinking more carefully and less ideologically about privatization. It is just as obvious that it is unlikely to do so. That leaves the legislature to take on this role. Given the current political makeup of Congress, hearings on this issue are unlikely, because if they were open and honest they might show that foolproof protections for data and information systems are difficult or impossible to devise, that dividing responsibility between the public and private sectors has the potential to create new dangers, that the problem is serious, that information is highly valuable and personal, that misuse of data and information systems can wreak havoc, and that there are serious consequences if it falls into the wrong hands – and that, therefore, it should not be subcontracted.

But if Congress were to do the right thing and immediately hold hearings on protecting information and information technology without a predetermined end, what issues should those hearings include?

First, it is not enough to bring on a parade of good guys. It is certainly true that contractors who have access to or store confidential information do realize they need to give confidential information a high degree of security.[79] In addition, some may be bound by codes of professional conduct. However, you cannot make public policy based only on the conscientious and competent.

Since as many government functions as are contracted out are contracted back in each year,[80] we have to plan for contract termination and its consequences. At a bare minimum, the contract must include the terms upon which the service will be terminated. In the case of information, this means creating and requiring a fully effective method for determining that all copies of information have been returned. Among those terms must be agreement as to ownership of data. It is hard to imagine any reason why those terms should give ownership to the contractor. But it may be that the contractor will assume it gets ownership and base the contract price on that assumption. In that case, the government may have to pay for the right to retain that ownership. In no case should the issue of ownership simply be assumed.

78. *Id.* at 533-34.

79. Policy Studies <http://www.policystudies.com/markets/child_support/elink_sub.asp>.

80. *See* Warner, *supra* n. 70.

Not only is there a need to provide for how information will be treated at the end of a contract, but, given the high degree of sensitivity involved with information handling and retention, there must be continuing oversight in order to protect information and to assess whether the contractor is performing properly.[81] In order to exercise oversight, to maintain full control of policy and management, government must retain and upgrade the necessary expertise.[82]

The problem is that recent managerial decisions are destroying this capacity. For example, when the Goldsmith administration in Indianapolis privatized its Information Services Agency, it was left so debilitated in terms of personnel and financially, it had trouble functioning.[83] When Connecticut state employees charged that the governor refused to provide promised training to upgrade state employees' IT skills, the governor's office responded that the employees could have better paying jobs in the private sector.[84]

Starving public IT functions is a precursor to privatization. One important reason cited for contracting out IT is government's lack of up-to-date expertise.[85] But if there is inadequate IT capacity in-house, then contracting out is not a salvation -- rather, it is very dangerous. Study after study has shown that oversight is critical to holding privatization accountable, but also that it is the weakest part of subcontracting.[86] If that is true where government has a high degree of expertise, then we are likely to see serious problems arising from a lack of adequate oversight of information technology. Furthermore, it will be impossible to hide this weakness from the contractor and its employees, who will know they have a free hand.

Congress – and we – must rethink whether conceiving of government in the mold of private sector organization is accurate and appropriate. Under that model, a successful business focuses on its core functions and outsources all others. It is this model that says information collection and retention is a private sector function and is

81. *See* Harold W. Demone, Jr., *The Political Future of Privatization*, *in* I The Privatization of Human Services: Policy and Practice Issues 228-30 (Margaret Gibelman & Harold W. Demone, Jr., eds. 1998).

82. *See e.g.* McDougall, *supra* n. 7.

83. Paul Annee, *Policing the 21st Century City*, *in* To Market, To Market: Reinventing Indianapolis 159, 169-70 (Ingrid Ritchie & Sheila Suess Kennedy, eds. 2001); Demone, *supra* n. 81, at 205, 206; *see* Lamont J. Hulse, *Targeting Neighborhoods*, *in* To Market, To Market: Reinventing Indianapolis 175, 190 (Ingrid Ritchie & Sheila Suess Kennedy, eds. 2001).

84. Welsh, *supra* n. 49.

85. Dannin, *supra* n. 53, at 45-47.

86. *Contract Management: Improving Services Acquisitions*, Statement of William T. Woods, Acting Director Acquisition and Sourcing Management, GAO-02-179T 1 (GAO Nov. 1, 2001).

not part of a government agency's function. But this model fails to take into account a government's relationship to those who elect it to govern them. Privatization excludes the public from input into decisions that affect individuals and the public welfare. It also fails to account for the dire consequences that may befall information once it is out of the government's sole control. All this suggests that it is time for government to upgrade and retain IT skills and to treat retention and collection of information as a core government function. It also means that background checks need to be performed on all employees handling information and performing IT functions.

Congress also needs to consider that if we have allowed our information infrastructure and capacity to deteriorate to the point that the only solution is privatization, we have been left vulnerable to hostile attack by hackers and even more malicious people. Logically speaking, this critical government function should not be allowed to deteriorate through neglect. But the failure to properly fund and staff this critical function appears also to undermine the intent of the *Privacy Act of 1974* and even to violate its specific mandate that agencies are to "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[87]

A recent General Accounting Office study found widespread collection and use of private information and Social Security numbers by many private companies. These are used for identification and to accumulate information about customers, but their collection and availability create a danger of diversion and misuse. The study concluded, though, that federal and state laws that restrict private companies from disclosing and gaining access to this information are important steps in safeguarding the public. [88] Experience with laws such as these are an important guide in how to

87. 5 U.S.C.A. § 552a(e)(10) (2003). *See* Privacy & Confidentiality, American Statistical Association's Privacy, Confidentiality, and Data Security Website <http://www.amstat.org/comm/ cmtepc/index.cfm?fuseaction=1> (containing a collection of articles on standards for maintaining confidentiality of data collected by government and used for statistical purposes).

88. H.R. Subcomm. on Soc. Sec., Comm. on Ways and Means, *Social Security Numbers: Private Sector Entities Routinely Obtain and Use SSNs, and Laws Limit the Disclosure of This Information* (January 22, 2004) (report to the Chairman, U.S. General Accounting Office) (available at <http://www.gao.gov/new.items/d0411.pdf>) .

take effective action to protect the public.

Along with that inquiry, Congress can consider whether more information is collected than is needed. In fact, government agencies are already required to do this under the *Privacy Act of 1974*. It states: "Each agency that maintains a system of records shall – (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President."[89] Congress should reassess whether this requirement has been complied with.

While this might identify some overreaching, the reality is that who else but the government should have data that includes our social security numbers or our history of social service usage. Government performs such a wide range of services, government as a whole must collect and retain a correspondingly wide range of data. Part of the investigation can be to ascertain whether private use of this data should be limited. The social security number is the primary problem. Social security numbers would have virtually no significance were it not for their overuse by private businesses as universal identifiers. This appropriation of the social security number for a private purpose has made it possible to bring the economy to its knees. Imagine the level of social and economic chaos that would ensue were only a small percentage of social security numbers to be compromised. Those individuals and their financial institutions would have to focus on their individual accounts. But the damage would be far broader. Consider the panic that followed the discovery of a very small amount of anthrax exposure. Many multiples of those individuals whose identities were stolen would be checking their financial records for problems. All institutions that use social security numbers or who deal with institutions that use social security numbers would have to deploy workers to deal with the crisis. The economy would come to a standstill.

If government is to contract out information and IT, it needs to identify and include the full costs of harm from their misuse when it costs out subcontracting. It must also be willing to pay for protections that will ensure to the greatest extent possible that information is not stolen or misused. This should include requiring that all nongovernmental and governmental employees handling public information hold high-level security clearances. The Treasury Inspector General for Tax Administration found: "Because these contractors are commonly given access to IRS computer systems and, in some cases, taxpayer data, they should be held to the same security

89. *Id.* § 552a(e)(1).

standards and procedures as IRS employees. Without sufficient oversight, the involvement of non-IRS employees in critical IRS functions adds to the risk of misuse or unauthorized disclosure of taxpayer data and could lead to loss of equipment or sensitive taxpayer data through theft or sabotage."[90]

Congress should also consider what criminal and civil sanctions will be adequate to prevent misdeeds, and it must develop and fund the means to track down wrongdoers. Although the *Privacy Act of 1974* provides criminal penalties that apply to contractors, they are far too limited. They make its violation a misdemeanor and subject to a fine no greater than $5000.[91] This is hardly sufficient compared with the gains to be made – either by those seeking financial advantage or terrorist ends.

Congress should consider the importance of bolstering whistleblower protections for employees of subcontractors as well as federal employees as a way to prevent wrongdoing or make it more likely perpetrators can be brought to justice. It is always difficult for an employee to report wrongdoing. Whistleblower laws are designed to stiffen workers' backbones so they will act in the public interest. Of course, providing greater protections to federal employees goes against the President's desires, now law under the *Homeland Security Act*, to decrease federal employee protections.[92] Private sector whistleblower protections have been left to the states to develop; however, rather than legislation directly giving whistleblower protections to private sector employees, Congress could require that federal agencies who subcontract must include meaningful whistleblower protections among

90. Treasury Inspector General for Tax Administration (TIGTA) TIGTA Audit Report #200320010 (Reference #2004-20-063), *Insufficient Contractor Oversight Put Data and Equipment at Risk* (quoted in Greater Oversight Needed for IRA Contractors, TIGTA Says, 200 Tax Notes Today 143-69 (Jul. 26, 2004)). That report also recommended limiting contractor access to IRS systems only to the extent needed to perform their tasks; monitoring their activities using audit trail analysis; and limiting software developer access to operating equipment. *Id.*

91. *Id.* §§ 552a(i), (m).

92. Richard W. Stevenson, *The Incredible Shrinking Government, Bush Style*, N.Y. Times § 4, 4 (Dec. 8, 2002). The recent enactment of the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (No FEAR Act), 5 U.S.C. 2301, et seq. (2003), which became effective October 1, 2003, provides remedies that are so weak it seems unlikely that it can be effective in encourage public employee disclosure of wrongdoing. It requires federal agencies to reimburse the government's judgment fund for all monies paid as court-ordered awards or in settlement of discrimination and whistleblower claims. A General Accounting Office report issued April 28, 2004 concluded that it is unlikely that the Treasury Department will be able to collect any more than 20 percent of the money it is owed. The Bureau of Natl. Affairs, *Federal Employees: Judgment Fund May Get Only $ 1 out of $ 5 Owed in Agency Reimbursements, GAO SAYS*, 92 Daily Lab. Rep. A-5 (May 13, 2004).

the contract terms.

The Executive branch has announced plans to privatize 850,000 federal jobs, nearly half the civilian workforce, in order to save money and improve performance.[93] This has problematic implications for many but especially for safeguarding information and national security. But when one looks behind the superficial claims of pro-privatization ideologues and examines careful case studies of privatization, there is scant if any evidence either of cost savings or greater efficiency.[94] In fact, ensuring that contractor employees receive adequate pay and good working conditions may be necessary to help remove temptations the underpaid would have to divert and sell information. Under those circumstances, there may be no savings.

Congress can also enlist the public by providing individuals with the practical and legal means to sue contractors who misuse information. The role of private subcontractors in collecting information, particularly when their role is disguised as the acts of the government, raises special problems. If the information is misused, the private individual may find it difficult to seek redress. First, since she will be unaware that she dealt with anyone other than the state, she may have no way of tracking how private information was released. There may be a high degree of trust in the government agency not to misuse this information, a trust that might be lacking or lower had she known it was a private subcontractor who was acquiring and maintaining the information. As a result, some degree of disclosure, both to the person providing the information and the person whose personal information is provided, may be required. But the reality is that even if an individual harmed by the release of personal information could track down the perpetrator and sue them, would there be a remedy adequate to deal with the harm suffered.

Congress should also be ready for the possibility that a fair investigation of the subject would lead it to conclude that public information and IT functions should not be contracted out. Cost savings might disappear if private contractors were held to the highest security standards. In such a case, it would be cheaper for the government to keep IT in-house.

Even more important, Congress may see that no matter how stiff the penalties are, or how certain justice is, the danger that our privacy

93. *Id.*

94. *See* To Market, To Market: Reinventing Indianapolis, *supra* n. 53; Elliott D. Sclar, *You Don't Always Get What You Pay For: The Economics of Privatization* (2000); Roland Zullo, *Confronting the Wicked Witch and Exposing the Wizard, Public Sector Unions and Privatization Policy*, <http://www.workingusa.org/2002fall/parttext/confrontingthewickedwitch.htm> (accessed Oct. 7, 2003).

may be violated, on the chance it might save the government some money, is simply a risk not worth taking.