

## **Public-Private Partnerships, e-Government, and Privacy**

**November 2006**

Over the past several decades, governments have turned increasingly to public-private partnerships (PPPs) as one means of financing and maintaining infrastructure and providing public services in the face of budgetary challenges. Recently, this trend has extended to e-Government. All PPPs should be based on clear contractual terms and careful government oversight. PPPs require special attention to privacy when the service being provided involves the collection or use of personally-identifiable information. Privacy concerns can best be addressed by ensuring that the private sector partner is subject to the same limits on use of data that would apply to the government agency if it were still providing the service itself. With such attention to privacy, PPPs are a viable alternative for government agencies seeking to maintain or improve services to the public.

### **Public-Private Partnerships**

Basically, a PPP is a contractual agreement between a public agency (national, regional, state or local) and a private company to supply infrastructure assets or services that traditionally have been provided by governments. In a true PPP, the private sector partner not only stands to profit from a successful project, it also assumes some of the risk of failure.<sup>1</sup> (In contrast, under ordinary procurement or outsourcing contracts, the private sector vendor is likely to be paid the same price regardless of how successful the project is.)

When first conceived, PPPs were used mainly for physical infrastructure projects, such as prisons, hospitals, and power plants. More recently, governments have turned to PPPs in providing services.<sup>2</sup> In countries around the world, a particularly interesting part of this trend has been the use of PPPs to enhance e-Government services. See KPMG, Public-

---

<sup>1</sup> National Council for Public-Private Partnerships, "How Partnerships Work"  
<http://ncppp.org/howpart/index.shtml>

<sup>2</sup> See, e.g., "Public-Private Partnerships and the Role of State and Federal Legislation in Wireless Municipal Networks"  
[http://web.si.umich.edu/tprc/papers/2005/431/TPRC\\_Tapia\\_Stone\\_Maitland.pdf](http://web.si.umich.edu/tprc/papers/2005/431/TPRC_Tapia_Stone_Maitland.pdf).

Private Partnership Opportunities in E-Government (November 2002)  
[http://www.agimo.gov.au/\\_data/assets/file/19014/PPP.pdf](http://www.agimo.gov.au/_data/assets/file/19014/PPP.pdf).

TexasOnline is one successful example of a public-private partnership that uses a performance-based model to share the costs and benefits of providing enhanced public services. Launched in 1999 as the state's official e-Government site for state and local government, TexasOnline (<http://www.texasonline.com>) is a public-private partnership with BearingPoint (formerly KPMG). As of 2004, BearingPoint had invested \$23 million in establishing the portal infrastructure.<sup>3</sup> BearingPoint recovers its costs and earns a profit through a combination of user, subscription and premium service fees. The state receives a portion of the transaction fees generated by applications and filings processed online and BearingPoint keeps a share. According to the Austin Business Journal, by 2004, TexasOnline had generated \$1 billion in revenue for the state and was processing one million transactions per month.<sup>4</sup> Meanwhile, individuals and businesses enjoy the convenience and cost savings of being able to transact business with the state online.

### **Advertising and Government Services**

The use of commercial advertising in connection with government services is widely recognized as a valid means of generating revenue to support governmental goals. For generations, buses and subways have carried advertisements, the fees from which help keep fares low. Advertising can be an important element of public-private partnerships. Consideration has even been given to advertising on e-Government websites, and some experiments have already begun in that regard. The Maricopa County website, for example, contains links to commercial enterprises.

<http://www.maricopa.gov/Default.aspx> The UK, a leader in e-Government, has concluded "Over time, it is likely that advertising and sponsorship will become increasingly important as ways of funding the provision of information and services or developing websites." <http://www.cabinetoffice.gov.uk/e-government/Resources/handbook/html/1-3.asp>.

### **Privacy and e-Government**

Of course, governments in the course of providing services and enforcing laws necessarily collect and use a wide range of personally identifiable information. When governments outsource to private companies for provision of services, those activities may involve the handling of sensitive personal information. Privacy rules in general do not prohibit outsourcing of data processing involving personally-identifiable information. For example, private contractors play a lead role in administering three of the nation's largest public health insurance programs -- Medicare, Medicaid, and the Department of

---

<sup>3</sup> Texas Comptroller of Public Accounts, Window on State Government, "Increase Usage of Online Government Services," <http://www.window.state.tx.us/etexas2003/gg21.html>.

<sup>4</sup> Austin Business Journal, "TexasOnline Passes \$1B Mark," <http://www.bizjournals.com/austin/stories/2004/04/26/daily13.html>.

Defense's TRICARE program -- handling sensitive medical records of tens of millions of patients.

A simple rule can address most of the privacy concerns associated with outsourcing: the private sector vendor should be subject to the same privacy and security rules that would be applicable to the government if it kept the entire process in-house. The federal Privacy Act is typical: It expressly contemplates the use of private contractors to collect, store and process personal information on behalf of the government and states that a contractor carrying out a government function involving the processing of personal information shall be subject to exactly the same requirements as apply to the government entity that issued the contract.<sup>5</sup>

On the issue of security, it seems clear that government agencies are no more or less reliable than commercial entities: all across the board, custodians of personal data need to improve their security practices. Breaches since 2005 seem to be fairly evenly spread among government agencies, for-profit corporations, non-profit entities and universities (both state and private). <http://www.privacyrights.org/ar/ChronDataBreaches.htm> Indeed, at least one commenter noted that the private sector has been more responsive to the needs of individuals after data breaches than the Veterans Administration was when it suffered on e of the largest data breaches ever earlier this year.<sup>6</sup>

### **Case Study: Motor Vehicle Registration Renewals**

A program currently being implemented in the US touches on all four issues discussed here: increasing reliance on PPPs, advertising-supported government services, the advantages of e-Government for citizens and governments alike, and the importance of protecting privacy. Imagitas, a Massachusetts company, has contracts with six states to prepare and mail notices alerting motor vehicle owners that they need to renew their registrations. The mailings include advertisements reviewed and approved by the State and generally related to motor vehicles. Imagitas prints the notices at no cost to the state, the states pay the postage, and Imagitas shares revenue from the advertisers who pay to have their material included in the mailing. Moreover, the mailings promote online renewal, which result in further cost savings to the states.

---

<sup>5</sup> “Government Contractors --When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.” 5 U.S.C. §552a(m)(1).

<sup>6</sup> Bob Sullivan “Vets Deserve Better Treatment After Data Theft,” Red Tape Chronicles (May 22, 2006) [http://redtape.msnbc.com/2006/05/vets\\_deserve\\_be.html](http://redtape.msnbc.com/2006/05/vets_deserve_be.html)

The program has several features that protect the privacy of personal data. Advertisers do not receive any personally-identifiable information. As under many direct mailing programs, the advertisers provide their advertisements to the mailer (in this case Imagitas) who mails them to appropriate recipients, but the mailer does not disclose its list to the advertiser. (In the purely commercial context, mail service companies do not disclose their mailing list to an advertiser since the list has value to the mailer, which would be lost if the list were disclosed to the advertiser. In this case, Imagitas makes no other use of the DMV list, and the advertiser understands that it cannot see the mailing list.) Imagitas does not commingle the DMV lists with other data. In targeting the ads, Imagitas does not seek to determine anything about motor vehicle owners other than what is disclosed in the DMV registration itself: make, model, year, purchase date and owner's Zip Code.

The federal Drivers Privacy Protection Act or DPPA, 18 USC §§ 2721 – 2725, is a prime example of privacy legislation that accommodates public-private partnerships while protecting privacy. The DPPA regulates the disclosure of personal information contained in the records of state DMVs; the Act *permits* DMVs to disclose personal information from motor vehicle records for a number of purposes. The drafters of the DPPA were careful to both permit the use of private sector contractors and to make it clear that those contractors were subject to the Act's requirements.

Thus, subsection (a) of the DPPA leads off by stating:

“(a) A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity ...”

Then, under “Permissible Uses” in subsection (b), the DPPA goes on to provide that protected information may be disclosed for a number of purposes including “For use by any governmental agency ... in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.”

It is 2721(a) that covers the Imagitas PPP: It clearly assumes that DMVs will use contractors to administer their programs (including PPPs, since a PPP is a contract-based arrangement). Under 2721(a), the use of a contractor is not even a disclosure; the contractor stands in the shoes of the government, and bears the same privacy responsibilities as the DMV. Similarly 2721(b)(1) recognizes that a DMV or other government agencies that receive DMV data to carry out their functions may also use contractors to process that data, so long as those other agencies or their contractors do not disclose the data for a purpose not permitted by the Act.

Thus, it is clear that the drafters of the DPPA were remarkably forward looking in recognizing the role of the private sector in contracting or partnering with DMVs in order to provide services. The DPPA permits the private sector partner of the government to do with data whatever the government could have done; conversely, the DPPA requires that contractors and partners be subject to the same limits as the government.

In this case, the private vendor does no more or less than the government could do on its own. Surely, a DMV would be able to include advertisements in its mailings to motor vehicle owners as a way of generating revenue to defray the costs of the mailings. It seems equally clear that the DMV could target the ads using Zip Code or make and model of automobile.

The marketing prohibition of the statute, subsection (b)(12), does not prohibit PPPs involving the use of advertisements. This provision of the Act was intending to prohibit the sale of DMV data to *third parties* for bulk marketing to individuals without their consent. The harm the DPPA seeks to prevent is the improper disclosure of the data. The Act does not prohibit DMVs themselves, already in lawful possession of the data, from using their data for marketing. And the same holds true for contractors acting on behalf of the DMV.

### **Conclusion**

Governments looking for innovative ways of improving services to their citizens might consider public-private partnerships. In using PPPs, governments need to pay careful attention to the privacy and security of personally-identifiable information. Best practice would be to ensure by contract that the data not be redisclosed or used for other purposes and that it be given protections at least equal to those that would have been provided if the data remained in the government's hands. The federal Privacy act and the Drivers Privacy Protection Act are examples of privacy laws that allow the use of private contractors to handle personal data of citizens, while requiring that the private contractors protect the privacy and security of the data just the same as the government would.

For more information contact: Jim Dempsey (202) 637-9800 [jdempsey@cdt.org](mailto:jdempsey@cdt.org). Mr. Dempsey was assistant counsel to the House Judiciary Committee at the time the DPPA was enacted.