
© Copyright 2009 IEEE
Commercializing Public Sector Information

Privacy and Security Concerns

MARK BURDON

The enhanced development of information and communication technologies in government has created new opportunities for agencies to collect, share and re-use data. At the same time, the commercial worth of governmental data sets and value-added information products/services have increased [1]. Government agencies are finding that data they have routinely collected to fulfil their statutory and business functions can now more easily be re-used for commercial purposes [2].

The prospect of increasing revenue through the commercial re-use of public sector information (PSI) is clearly appealing for governments and their agencies. Examples of PSI that have been re-used commercially include residential property transaction details, land title information, ordnance survey data and street address registers. However, the commercial re-use of PSI raises a key question about the technocratic
public administrations of the future: what happens to e-government organizations when they move from being service providers to market-oriented, income generators? This change could generate a re-balancing of government priorities, a rebalance that will favor income generation policies over previously held democratic norms that defined the scope, nature, and boundaries of the relationship between governments and their citizens [3]. Moreover, a paradigmatic change of governmental ethos could also raise security concerns. The enhanced publication of PSI, particularly for income-generation purposes, could lead to conflicts within and between government agencies regarding the restriction and distribution of information.

These shifting priorities become more apparent when the commercial re-use of PSI is considered in the context of the information privacy legal obligations placed upon agencies. Ultimately, the shifting boundaries will influence the shape of and prospects for a transparent and open information society, which in turn will influence notions of national security.

This article examines those shifting boundaries, particularly in light of information privacy and national security concerns arising from governmental commercialization of PSI that includes personal information. I seek to show that information privacy laws can be subverted in the face of overt commercialization by government agencies; that commercialization can have a negative impact on individuals; and can also give rise to societal concerns relating to privacy, security, and the open governance of the information society.

Reuse of PSI

The re-use of PSI reflects the important role that governmental information dissemination has with regards to the functioning of open, civil societies. Dissimilar political perspectives have different priorities regarding the conceptual underpinnings of PSI re-use that can be categorized by two competing public goods: open access to government information and the re-use of PSI as an income generator for both the public and private sectors.

Existing re-use policies encapsulate both of these competing goods in an attempt to balance the complexities of governmental information dissemination, particularly via commercialization strategies. This competing balance results in policies that have clear philosophical statements about their intent that is not necessarily matched in clarity by the application of day-to-day practices, as evidenced in the approaches adopted by the EU, the U.S., and Australia.

First, it is important to acknowledge the unique position that governments have as a collectors of public data [4]. Agencies have statutory means to enforce disclosure and they are the only feasible providers of comprehensive national data sets [5, p. 227]. Nonetheless, defining PSI is not a simple task due to the inherent tensions between a citizen’s right of public access to government information and the economic benefits that arise from the commercialization of public sector information [6, p. 2]. These philosophical differences are evident in the commercial re-use of PSI policies that have been developed in the EU and the U.S.

During the course of the last two decades, EU policy objectives have defined PSI in different ways to reflect different policy and economic ambitions [7]. The first attempt to instigate an EU-wide policy on PSI was developed in 1989 [8]. It sought to synthesize public and private sector initiatives to stimulate economic growth in a Europe-wide information market.

The European Commission attempted initiatives during the next 13 years, and the commercial re-use of PSI remained on the policy agenda [9]–[12], despite the inherent political, administrative, and technical complexities of developing an EU-wide strategy, such as different national administrative rules, digital formats, and pricing regimes [13, p. 195].

In 2003, the Commission implemented “Directive 2003/98/ec of the European Parliament and of the Council of 17 November 2003 on the Reuse of Public Sector Information,” to encourage the commercial re-use of PSI throughout the EU member states [8]. The Directive provided a governance framework to alleviate the problems encountered during the previous decades. The Commission’s economic intent was established via a general principle of commercial re-use, namely “whenever public sector information is generally accessible, commercial re-use should be considered.” However, the commercial re-use of PSI was still left to the discretion of member state governments which made it virtually impossible to implement a unified, EU-wide PSI framework [14, p.12].

The Directive was also solely concerned with the public sector and no conditions were placed upon private sector information brokers [14, p. 12]. The Directive also created income generation opportunities for government agencies by allowing public sector bodies to make profits from the commercial re-use of their PSI [15, Art. 14]. Government agencies could therefore attempt to recover costs as long as any charge was a “reasonable return on investment” and was not “excessive.”

The Directive has come under some criticism. For example, Blakemore and Craglia [6, p. 3] state that the Directive is “based on an untested assumption that there is a latent demand for information that is unfulfilled because of technological and policy ‘barriers’ that therefore need to be removed.” Several authors have also criticized the overt economic interests of the EU’s policies which overshadow
Government policies balance open access to government information with considerations about the role of the private and public sector in the information economy.

the information access rights of citizens [7], [14], [16], [17]. As such, the commercial re-use of PSI is a market-oriented approach that has a rationalistic and linear viewpoint that overly focuses on technologies, information, and benefits but does not encapsulate the true complexities of the situation [6, p. 3].

The policy situation in the U.S., at least at the Federal level, is somewhat different. Unlike the EU, the dichotomy between the commercial re-use of PSI and the information access rights of citizens does not exist [18, p. 3]. The vast majority of Federal Government information is freely available to the private sector and the public. The purpose of this approach is to ensure that taxpayers do not pay twice for government information and to encourage the widest possible dissemination of information [16], [19].

Four existing laws form the PSI foundation of the U.S. Federal Government [20, p. 123]. The First Amendment of the U.S. Constitution guarantees freedom of speech and promotes open political dialogue. The First Amendment does not specifically preclude the Federal Government from commercially re-using PSI but it sets a tone for prohibiting government interference in the marketplace that has been followed by subsequent pieces of legislation [21], such as, rule 34 of the Copyright Act 1976, which expressly prohibits copyright protection of Federal Government works. The effect of the legislation is to place all Federal Government information in the public domain [21]. The public interest is served "by keeping governmentally created works as free as possible of potential restrictions on dissemination" [20, p. 126]. However, the prohibition of copyright does not extend to state governments who are allowed to copyright their data and can therefore commercially re-use information held by them.

The U.S. Freedom of Information Act of 1966 ensures public access to government information. The Act permits any person to request any record in the possession of a federal agency in order to establish a culture of disclosure for government records [20, p. 124]. In 1996, amendments were introduced to reflect technological changes and the advent of electronic record-keeping. Accordingly, if an agency receives three or more requests for the same records, it is obliged to make the information available on its website thus adding a wider information dissemination purpose to the public access aims of the legislation [20, p. 125]. The final piece of legislation, the Paperwork Reduction Act 1995, aims to prevent bureaucratic control of information by directing agencies to ensure that information is disseminated to the public in a timely and equitable manner. A key purpose of the legislation is to ensure that government does not have a monopoly over its information and thus prevents an agency from commercially re-using its own PSI [20, p. 130].

The Australian situation, again at the Federal level, is philosophically less clear-cut as there appears to be no coherent or overriding PSI policy agenda. The "Intellectual Property Principles for Australian Government Agencies" [22] provides "a broad policy framework for intellectual property management" that covers a wide range of works produced by the Commonwealth. Agencies are nonetheless encouraged to develop their own individual intellectual property management frameworks that reflect their own needs and objectives. While the principles provide an overarching guideline for Commonwealth agencies, the ultimate form of implementation is left to the agencies themselves.

The Australian Principles 11 to 15 are particularly relevant to the issue of commercializing PSI. Principle 11 states that agencies “should encourage public use and easy access to copyright material” that is primary to the function of government. This is similar to the access right provisions of both the EU and the U.S. which deem fundamental government information should be made freely available. However, the use of the words "should encourage" is by no means as strong as the obligations that U.S. Federal Government agencies must comply with. Principle 13 states that Commonwealth agencies should be responsive to opportunities for commercial use and exploitation of intellectual property. Furthermore, agencies should consider the potential benefits that may be realized through commercialization opportunities with the private sector. The Intellectual Property Principles recognize the importance of making core government information freely available (like the U.S. and the EU) and offer a watered down version of the EU’s marketization strategy.

In summary, policies regarding the commercialization of PSI differ. Policies are marked by philosophical underpinnings that balance open access to government information with considerations about the role of the private and public sector in the information economy.
Considerations about the information economy can transform traditional notions about the role of government as an information disseminator, a transformation that can give rise to privacy and security concerns.

Information Privacy Concerns

A difficulty arises for government agencies considering the commercial re-use of PSI: the principle of consent is fundamental to information privacy and data protection laws. Information privacy laws consign upon data collectors various constraints that govern the collection, use, and dissemination of personal information. Information privacy ensures that information about an individual is kept confidential and is only used for purposes to which that person has consented [23]. Within the context of governmental commercialization of information, an analysis of information privacy issues is integral to resolving the tensions of trust that arise from enhanced use of technologies by governments and the anxieties of citizens regarding the use to which their personal information is put [24, p. 13].

These tensions are likely to arise in commercialization because personal data will be used for a different purpose than that for which it was collected, namely governmental income generation. In the case of commercialization of PSI, the “primary purpose” of data collection fulfills the agencies’ legislative obligations and fulfills an essential administrative function of the agency. However, when an agency attempts to commercially re-use its information, including personal information, either as raw data or as value-added information/product, it does so for a “secondary commercial purpose.” An individual has consented to the primary purpose, but may not have consented to, or even been aware of, the secondary commercial purpose thus exacerbating those tensions of trust highlighted above.

Do government agencies have the legal right to collect and to re-use personally related information for income generation purposes? The key concern is whether agencies can legitimately claim a secondary commercial purpose for re-using personally related information, either via the consent received from individuals or from an existing legislative exemption. Two examples of PSI re-use problems from the U.S. and the U.K. highlight the tensions between citizens and government agencies regarding the re-use of personal information for income generation purposes.

In the 2005 U.S. case Kehoe v Fidelity Federal Bank & Trust [25], a class action was brought against the Fidelity Bank regarding its purchase of 565,600 names and addresses from the Florida State Government’s Department of Motor Vehicles (DMV). Upon purchase, the Bank used the DMV’s information to mass mail Florida residents about car loan advertisements. This act was in direct contravention of the Federal Drivers Privacy Protection Act (DPPA) [26], which requires state governments to protect the privacy of an individual’s personal information contained in motor vehicle records.

The DPPA was enacted in 1993 to deter would-be stalkers from gaining access to victims via publicly listed motor vehicle records. A further amendment was enacted in 1999 that required a state DMV to obtain the consent of any individual whose driver license was being sold for bulk marketing purposes. In the Kehoe case, the plaintiffs’ consent was required before the DMV could re-use and sell their information to the Bank. However, the 1999 amendment, which was enacted in 2000 by the Florida legislature, was never updated into Florida law due to an oversight. As such, driver license information continued to be used for commercial purposes without consent. The U.S. District Court for the Southern District of Florida found for the Bank at first instance because the plaintiffs could not demonstrate that the Bank’s breach of the DPPA caused them actual harm. The plaintiffs appealed to the 11th Circuit Court of Appeals and the court overturned the decision holding that it was not a requirement under the DPPA to prove actual harm for a claim of damages. The Bank was required to pay $US$50 million to the plaintiffs for using their personal information for marketing purposes without their consent.

Also in 2005, the U.K. Government’s Driver and Vehicle Licensing Agency (DVLA) encountered problems selling driver license information. The DVLA is responsible for collecting data on persons who have been issued a U.K. driving license and for vehicles registered within the U.K. For a small sum, the DVLA routinely sold its driver license information to certain companies related to the regulation of parking offences, such as car park managers and car clamping firms. For an extra charge of around £3000, the DVLA authorized direct access to its database system which allowed companies to type in a registration number and to download corresponding personal information about the registered car owner [27]. The DVLA claimed that it was obliged to commercially re-use its PSI because of a 2002 statutory instrument that required the organization to sell information to anyone with “a reasonable cause” [27].

Despite the fact that only companies with a reasonable cause were supposed to access the DVLA’s database, the agency authorized access to one of Europe’s largest credit card companies, who are were known to employ extensive direct mailing tactics, on the pretense that the company had a reasonable cause because it owned a private car park at its central office [28]. More
worryingly, the DVLA also sold its information to a private car clamping firm whose directors were found guilty of blackmailing unsuspecting motorists. The blackmailers sent threatening letters to victims citing their registration details and claiming that a spurious parking violation had taken place [27]. Subsequent critical media coverage about the DVLA’s commercial activities led to the Department of Transport, which houses the DVLA under its accountability framework, to respond by establishing a public review and consultation exercise [29]. The review resulted in 14 new measures including detailed guidance on what constitutes a reasonable cause, a requirement for organizations to be members of an accredited trade association and the instigation of a new complaints procedure.

Several points of interest arise from the Kehoe and the DVLA examples. The construction of the DPPA is unusual in the context of information privacy and data protection laws. The DPPA was established to deter would-be stalkers and it therefore obliges the buyers, rather than the collectors (or sellers) of data, to act within certain confines. As such, in Kehoe, an action was brought against the Bank but no action was brought against the Florida DMV. Contrast that with the DVLA example, where the agency received valuable criticism that resulted in a consultation review of its actions and the implementation of stricter guidelines to correct its information re-selling practices.

Both examples provide different methods of obtaining consent but both failed to supply an effective means of privacy protection regarding the commercial re-use of personally related PSI. For example, section 2721 of the DPPA indicates the purposes for which motor vehicle records can be used. This includes a provision for mass mailing solicitations if the information provider has obtained the express consent from the individuals named in the mailing list. If an individual has not provided consent to the release of his/her motor vehicle record for the purpose of mass mailings then the DPPA prohibits the use of their data in that specific way [30]. In the Kehoe case, the consent requirement was inadvertently not enacted and the DMV continued to sell its information without restriction.

In the DVLA example, only interested parties (i.e., those with a reasonable cause) should have been able to gain access to a driver’s personal information. However, as detailed above, the practical definition of “a reasonable cause” was so broad that it allowed illegitimate access by companies, and once information was accessed, there was practically no restriction placed on the use of the information. The implicit assumption behind the DVLA’s commercial actions was that individual drivers had consented to any re-use of their information. This was clearly not the case as witnessed by the widespread criticism heaped on the DVLA after the media broke the story.

Both cases represent a failure of government agencies to obtain individual consent for a secondary commercial purpose. This illustrates a disturbing lack of concern for information privacy issues that arise from governmental commercialization of personal information and for the potential negative effects on individuals.

National Security Implications

The Kehoe and DVLA examples underline information privacy concerns at an individual level. National security concerns also arise from the commercialization of PSI at a governmental and societal level.

It is worth noting just how cheaply personal information was being sold in both cases. In Kehoe, the Bank paid $US5656 for the personal information of more than half a million Florida residents which approximates to only one cent for each name and address they bought. The DVLA sold details of individuals for only £2.50 per record. Nevertheless, the DVLA earned £6.3 million in 2005 from its commercial re-use of personal information [31] which gives a clear indication of just how many records were routinely being re-used and sold. Furthermore, evidence from the U.S. has also suggested that state-based DMV’s have been susceptible to fraud, corruption, and weak security practices [32]. For example, in December 2003 a former state employee from the Nevada DMV pleaded guilty to receiving bribes totaling more than $US300 000 to provide unauthorized identification documents to illegal immigrants. In June 2002, 36 people, including DMV staff, were indicted in a complex criminal operation that involved the fraudulent issue of New Jersey driving licenses. The criminals involved were so sophisticated, and the demand so great, that different brokers competed against each other to provide the best choice of illegal services at a price to suit [33].

These cases show the commercial value of driving license personal information. In the case of the “legitimate” sales of the Florida DMV and the DVLA, the commercial value exists because of the potential uses for which third parties can utilize the information through direct marketing. In the case of fraudulent or other criminal acts, a commercial value exists for the provision of fraudulent identification that can be used to dishonestly confirm a false identity. Although the reasons behind the agency sales and the criminal acts are very different, they nonetheless provide consequential threats for national security because both situations provide greater access to the fundamental material of identity theft—personal information that can, with relative ease, be recycled.
into a fraudulent identity. In fact, it is astonishing at a time when identity theft is fast becoming a major crime concern in most first world countries, that both agencies were selling personal information at basement store prices, and more worryingly, paid scant regard to whom they were providing it. It would appear from the two examples highlighted, that commercial reasons, whether directly or indirectly, outweighed the potential threats of national security arising from the misuse of personal information for identity theft crimes.

Issues regarding the governmental commercialization of personal information, particularly driver license data, may therefore impact upon national security concerns. While governments have recognized the security issues arising from the identification purposes of drivers’ licenses, they have not been as quick to recognize the concerns that may arise through the commercialization of driving license information. Legislative and technical responses have tended to focus on the construction of more robust forms of license that can be used for identification purposes, as exemplified by the Real ID Act in the U.S., and the Queensland Smart Driving License in Australia. However, the personal data from licenses has been, and continues to be, sold to commercial entities and other bodies.

This situation creates a paradoxical situation. Governments throughout the world are setting aside large amounts of financial, legislative, and technical resources to create stronger forms of driver license identification. Yet the information behind those licenses is commercially available at inexpensive prices. As highlighted above, the DVLA received just criticism regarding its commercial practices that infringed on individual privacy and that provided foundational support for criminal fraud. Those same criticisms are equally applicable to national security concerns.

The principle of consent is fundamental to information privacy and data protection laws.

It should also be recognized that governmental commercial transactions with legitimate sources (e.g., information brokers), still give rise to national security issues, due to the reduction of control that government agencies have over information once it has been sold to a commercial third party. While a government agency can license certain uses that its information should and should not be put to, the ultimate decision about whom a commercial third party sells information to resides with the third party. It also has to be acknowledged that there are potentially less stringent checks and requirements imposed on a private sector information broker in comparison to a public sector, government agency. In effect, once governmental information is distributed for sale, it is difficult for governments to control to whom it is ultimately sold, or to restrict its use. That said, it is clearly unacceptable for a government agency to provide, let alone sell, personal information to an illegal or illegitimate source.

Privacy and National Security Issues

The Kehoe and DVLA examples highlight the volume of PSI that is commercially re-used for governmental income generation purposes. This raises implications for the prospect of an open, transparent, and secure information society. A balancing of societal interests is required which reflects the differing priorities within governments and their effects on individuals. On one side of the scale, we have the societal interest arising from access to government information whether it is in the form of free and open access to enhance democracy, or whether it is in the form of the commercial re-use of PSI to enhance the information economy. On the other side, we have the societal interest arising from the trust relationship between citizens and their governments, a relationship which is founded upon the keystone notion of information privacy. Both interests represent competing values involving the requirements of economically self-sufficient governments to sell, restrict, and distribute their information versus the individual citizen’s right to access and to control the use and re-use of their personal information. The complex reconciliation of these interests is further compounded when issues of national security are added to the mix.

It is easier to identify the conflicting societal interests entailed in the commercial re-use of PSI and the information privacy of citizens than it is to harmonize these competing concerns, especially in light of national security issues. A balance will not be found by simply examining and updating PSI, information privacy and national security legislation. Current laws do not adequately reflect the conceptual complexity and the democratic importance of maintaining a balance between open access to government information, governmental income generation through the commercial re-use of PSI, the information privacy of citizens, and the national security requirements of governments.

All of this requires government agencies to pay careful attention to privacy and national security issues when making decisions to commercialize PSI held under their custodianship. Both the Kehoe and the DVLA examples highlight concerns that can arise from the
commercialization of PSI and the negative consequences that can emerge for government agencies that have an overt income generation outlook. The advent of widespread identity-related crimes and increased terrorist threats place greater requirements on government agencies to think carefully before they adopt new PSI commercialization strategies or re-engage in existing commercial transactions. Otherwise advanced and unchecked marketization of government information could have a detrimental effect on both individual privacy and national security.

Author Information
Mark Burdon is a Ph.D. Candidate and Research Associate, Faculty of Law & Information Security Institute, Queensland University of Technology, Queensland, Australia; m.burdon@qut.edu.au.

References