eCitizenship and its Privacy Protection Issues

Dr. Christopher N. Carlson
IWF Wissen und Medien gGmbH, Göttingen, Germany
e-mail: christopher.carlson@iwf.de

Abstract: It is generally accepted that the global information society needs comprehensive and effective privacy protection in order to build trust and confidence on the part of its participants. This is most especially true with regard to eGovernment. Current eGovernment concepts mostly require that prospective eCitizens reveal substantial amounts of personal data as the price of claiming their rights to eInclusion and eParticipation. The arguments in favor of this view are well known. This paper considers the reverse proposition: That the potential advantages in terms of enhancing citizens' trust in the benevolence of eGovernment (and thus of diminishing the current atmosphere of political discontent) greatly outweigh any abstract danger to the state in the form of individuals misusing the system. Online privacy protection policies and data protection laws need to be significantly upgraded. More resources should be committed to the enforcement of existing legislation and penalties and sanctions for privacy rights violations - both malicious and negligent - ought be tightened up.

Keywords: eCitizenship, eGovernment, privacy rights, privacy protection

1. Privacy rights

Privacy is widely recognized as a basic human right. The American jurist and later Supreme Court Justice Louis Brandeis wrote as early as the 1890s about “the right to be left alone”. (Warren and Brandeis 1890) Numerous international policy statements and frameworks for the information age state that individuals are entitled to fair and equitable treatment in the way that personal information is collected and used. This most assuredly includes personally identifiable information in the hands of government agencies. Government agencies are increasingly using the Internet as a means to deliver services and information. This development allows users to register for government services, obtain or file government forms, discuss public policy issues and generally engage in a growing number of other functions online. The trend towards e-government and the electronic delivery of services has significantly expanded government collection of personally identifiable data. In providing services to the public and carrying out various functions, governments collect and use a wide range of personal information about their citizens (such as health, education, employment and property ownership records, tax returns, law enforcement records, drivers license data, to name only a few). A government’s practices in collecting, retaining, and managing personal data about its citizens give rise to a wide range of privacy concerns.

Governments have the right (and also the duty) to write the rule book with regard to the power relationship between citizenry and government. From this basic fact, subsidiary right/duty-dualities are derived. This is particularly true in the case of liberal democracies, since these have a plain obligation to provide for a level playing field, and also to exercise considerable restraint with respect to citizens’ privacy rights, these being fundamental to a functioning democracy. It is also a fairness issue in that governments have the power to compel citizens to deal with them. At least in theory it is possible to refuse to deal with businesses which do not respect their customers’ privacy rights; as a practical matter this is not possible with governments.(Dempsey *et al.* 2003)

In 1980, the Organization for Economic Cooperation and Development (OECD) concluded that privacy protection was an important human right but that inconsistent national privacy laws might slow the realization of the economic and social benefits of the Information Age. An international team of OECD-convened experts developed a set of Privacy Guidelines, consisting of definitions, eight Privacy Principles, and possible enforcement approaches (OECD 1980). These guidelines were intended to offer uniform protection of individual privacy rights while being flexible enough to work under a variety of social, legal, and economic circumstances. The 1980 OECD Guidelines have had enormous influence, finding their way into a variety of legislative and self-regulatory adaptations.

In 1995, for instance, the European Union adopted its Data Protection Directive (95/46/EC), establishing a detailed privacy regulatory structure for adoption into national law by EU member states. This directive owes much to the OECD guidelines and was substantially influenced by them.

2. Privacy protection – lessons from the private sector

At the same time, online privacy protection policies and data protection laws need to be significantly upgraded. More resources should be committed to the enforcement of existing legislation and penalties and sanctions for privacy rights violations - both malicious and negligent - ought be tightened up.

Many countries now recognise the civil law tort of "invasion of privacy". As stated in U.S. law (*cf.* Restatement (Second) of Torts, Section 652A), this consists of four separate and distinct rights, or rather, the violation of these rights, as follows:

- the unreasonable intrusion upon the seclusion of another
- the appropriation of another's name or likeness
- the unreasonable publicity given to another's private life
- publicity that unreasonably places another in a false light before the public

These torts exist in some form of another, under common or statutory law, in the overwhelming majority of the U.S. federal states. (Vartanian *et al.* 2002)

These torts are – by their very natures – acts committed by persons against persons or by private organisations, e.g. corporations, against persons. However, it should not be overlooked that these four forms that invasion of privacy can take are, to some extent, also possible outcomes of state activity.

Certainly the first tort is a suitable metaphor for the seemingly unslakeable craving that some governments have to interfere in the lives of their citizens. The second tort is unlikely to be perpetrated by a state agency, except, possibly, within the narrow context of espionage agencies, but some countries – noteably the U.S. – have some rather extensive notions of what personally identifiable information may be provided to others in the form of public records. For example many – if not most – of the U.S. federal states maintain publicly accessible sex offender databases. The final tort on the list – placing someone in a false light – is also something that can occur as the result of state action. Take, for instance the case of the student Eleonore Poensgen, who was suspected by authorities in the 1970s of being involved in terrorist activity. Prosecutors gave her name to the media, some of which promptly published unwarranted smear stories about her. Although she was later absolved of any blame and won a major libel suit against a daily newspaper which had published the story of her alleged involvement in a particularly prominent manner, she may well still be listed as a suspect – or even as a fugitive at large – in the databases of law enforcement agencies in other countries. It is vastly more likely by several orders of magnitude that someone will be characterised as a suspicious person than that the later-arriving proof of their innocence will be as widely disseminated.

Data protection laws permit, facilitate or even mandate the commercial and governmental use of personal data while providing individuals with some degree of control over what they must disclose, information on how their personal data will be used, the right to demand that data shall be accurate and up-to-date, and protection with regard to personal information being used to make decisions about a person.

Though a person's interaction with the economy is to some extent voluntary, but not perhaps quite as voluntary as some commentators would have us believe, since – as a practical matter – only a comparatively small number of people can realistically live in log cabins and grow all their own food, even these interactions with private sector actors can point up the inherently invasive nature of cross-linked data which have achieved a certain critical mass.

In 2003, the International Chamber of Commerce explored the impact of regulation upon the growth of information age business and concluded that the 1980 OECD guidelines remain sufficient to protect individual privacy rights. In its Toolkit for Policy Makers, the ICC offers common sense advice, urging that privacy regimes be judged in terms of their practical effectiveness (ICC 2003). Unsurprisingly perhaps, the ICC favors privacy regimes that strike a balance between the competing interests of all stakeholders. Business-people – particularly those engaging in e-commerce – are among such stakeholders, as are, of course, the consumers whose personal data are sought for marketing purposes. The ICC considers that no greater deference is due the privacy rights of the individuals than to the right of businesses to exploit such data. Both rights sets are equally valid, equally important. The persons whose data are to be so used, not just by the business that originally acquired them, but also by anyone else to whom that business might care to sell them, may well hold markedly other views on this question.

The American Civil Liberties Union (ACLU) has a satirical online video[1] dealing with the potential dangers of cross-linked and networked personal data. A person trying to order a pizza for dinner is suddenly confronted by the pizza vendor's comprehensive knowledge of his financial and health care status, his vacation plans, what periodicals his wife subscribes to and much more as well. Though, as just stated, this video is plainly satirical in intent, there is little doubt that there is quite a lot of personal data available to the nosy in a remarkably short time-frame and for very little effort to be had from public records collections.

There is another reason why we should be concerned about data collection in the private sector: If businesses are free to buy and sell personal data collected from customers and/or culled from public records, then governments wil be free to purchase this information, too. There are indications that this is actually happening now in the U.S. According to a newspaper report, the U.S. Justice Department has an $ 8 million contract with the data mining company ChoicePoint which allows government agents to tap into its huge collection of personal data. (Simpson 2001) If, for example, insurance companies collect genetic data about their policy-holders, then it seems safe to assume that the same governments which are calling for the encoding of personal biometric data onto national IDs and passports will look for and almost certainly find ways to violate citizens' genetic privacy and acquire these data. The same applies to the RFID chips which will purportedly tell our refrigerators when it is time to order more milk, and which will also be able to provide whomever with comprehensive movement profiles about us.

3. eGovernment and the eCitizen

Current eGovernment concepts mostly require that prospective eCitizens reveal substantial amounts of personal data as the price of claiming their rights to eInclusion and eParticipation. The arguments in favor of this view are well known. This paper considers the reverse proposition: That the potential advantages in terms of enhancing citizens' trust in the benevolence of eGovernment (and thus of diminishing the current atmosphere of political discontent) greatly outweigh any abstract danger to the state in the form of individuals misusing the system. For instance, the frequently expressed concern about persons abusing the franchise to vote more than once per election seems disproportionate given declining voter participation so that voting fraud is unlikely to be such a large-scale phenomenon that it might corrupt the political process.

What is the underlying rationale for eGovernment? Unsurprisingly, there is no single rationale for eGovernment. One common agenda in the German eGovernment discussion is the simplification and modernisation of civil service administrative agencies, an issue mostly seen from the point-of-view of the agencies themselves, which is to say that the main stress is on making these easier for the agencies, rather than for the public. On the other end of the scale there are political agendas which hope for an enhancement of political inclusion and participation on the part of socially, politically or economically marginalised persons. Since these persons are, however, often on the wrong side of the Digital Divide, there is an element of unwarranted optimism in this.

[1] http://www.aclu.org/pizza/

A case in point – interestingly – comes from a recent election in Haiti. In the first national election since the Aristide government was expelled by a coup d'etat, prospective voters were required to get a new national identification card with individual biometric characteristics. This measure was actually advertised by the new provisional government as a means of extending the franchise to a large number of poor rural citizens who previously had had no state-issued IDs at all. The purported beneficiaries did not, however, flock in masses to enhance their participation and inclusion in the national political process (Schmidt 2005). Apart from the prohibitively high cost of such an identification document to the holder – biometric IDs are more expensive than traditional ones by a factor of several hundred per cent – citizens who have only just recently been subject to rule by a brutal and repressive dictatorship are not likely to have what one might call 'blind faith' in the benevolence of whatever government has happened to succeed the previous one. And the fact that this new government expects its citizens to provide it with biometric data is unlikely to make those same citizens more trusting: If anything, precisely the reverse can be expected.

What can be learned from this object lesson? Governments are unlikely to engender trust and confidence in the citizenry by treating them as if they are all potential or actual delinquents permanently on probation. Even if such treatment were in any way justified by excessively high crime rates – and the crime rates of most civil societies are gratifyingly low – this is not something the political establishment can fairly cast as a unilateral demand or commandment. It should be recalled that the government is hired help; the people are the sovereign, not the state apparatus.

The high-profile terrorist attacks on targets in the USA in 2001 had an unfortunate influence on the discussion of the biometric identification issue. Law enforcement and intelligence agencies have frequently succumbed to the temptation to co-opt these attacks to further their biometric agendas. It should, however, be recalled, that the terrorists involved travelled to the U.S. under their own names and with correct identity documents. The problem was that they were not known to be terrorists. This is now the standard paradigm for international terrorism. The ringleaders themselves either do not travel or they use wholly illegal means to do so. Those tasked with carrying out a terrorist attacks are persons having no known track record. These persons are sometimes - a term of implicit contempt - called "disposable terrorists", because they usually do not survive the one attack they carry out. Biometric identification systems are unsuited to identifying disposable terrorists and thus, by inference, in preventing their attacks. Counter-terrorist arguments are therefore not pertinent to the advocacy of biometric identity documents. (Jonas 2004)

4. Who trusts whom – and why?

It is generally accepted that the global information society needs comprehensive and effective privacy protection in order to build trust and confidence on the part of its participants. This is most especially true with regard to eGovernment. Where, if not in the state apparatus, is the potential for oppressive action against persons greater if personal information should be wrongfully acquired and/or abused?

There is a broad consensus that one of the main pre-conditions for development of the Information Society is for users to have confidence or trust in the reliability, security, and integrity of electronic communications systems and computerized information processing systems. Individuals will not readily use networks or systems they do not trust. In the absence of trust, individuals will refuse to disclose personal information, or they may well give false information. One central aspect of the trust framework is privacy protection – in other words credible assurances by means of law, technology design, and/or industry practice that personal information will be collected, exchanged and used fairly. Surely these are propositions we can all agree to without much in the way of quibbling.

Yet the common wisdom goes on to assert that – in this context - information privacy or data protection is not so much about keeping personal information secret; but rather it is about creating a trusted framework for collection, exchange and use of personal data in commercial and governmental contexts. (*Cf.* Global Internet Policy Initiative 2004)

Governments are responsible for identifying their citizens. There are several different reasons for doing this, such as in order to perform administrative tasks and to enforce laws which make a distinction between citizens and non-citizens. The citizens themselves have an interest in being state-identified, for instance if they wish to travel abroad. Possession of a passport - *ceteris paribus* - greatly facilitates entry into another country. Some passports may be more useful than others in getting into certain countries – an Israeli passport presumably is not an advantage for someone wishing to go to Saudi Arabia – but generally speaking some passport is better than no passport or a Nansen passport, now called a "Convention Travel Document" because it was created in 1951 by a UN Convention.

One way in which state identity management may be handled is by creating a central registry of all citizens (and thus, by implication, of all resident non-citizens as well) and issuing internal passports or other identity documents to them. This is not, however, actually necessary, and a variety of countries do just fine without internal passports or central registries of the citizenry. Citizenship can usually be inferred from documents such a birth certificates, residence can safely be inferred from a paid electricity bill. It is perhaps useful to recall that travelling statesmen routinely carry no identification whatsoever; their identity is presumed or inferred from indirect evidence such as his or her arrival in the president's aircraft or the fact that the ambassador of a certain country is seen to defer to a person who claims to be the president of that country. What is now a special privilege for members of government was once quite usual for everyone. Stefan Zweig remarked nostalgically in his memoirs that prior to 1914 he had travelled all over the world without having a passport at all and without ever seeing anyone else asked for one either. (Zweig 1944) Historically, the emergence of passports in Western societies dates from the 17th century, with Louis XIV of France issuing an edict in 1672 prohibiting departure of his subjects or entry of foreigners without an official letter of authorisation; sort of a Berlin Wall made of paper.

State identification may be defined as the sum of information about a person which the government has publicly certified as being correct. The state will usually also have much more data about a person than that which is stated on the identity document. Parentage, marital status, children born in or out of wedlock, criminal record, to name only some of the many possibilities may all be stored in state records systems. State officials and private persons or businesses will generally accept such state identity documents as *prima facie* evidence of a person's identity. Thus authenticated, the person may claim all the rights accruing to his or her identity, and must also perform all the duties incumbent upon him/her. The trust placed in these documents is based on the facts having been verified by disinterested third parties, i.e. the state. Also, the state only permits one identity per person. For instance in cases where a person who is a member of a religious order has a name recognized only by the order, the state may choose to take cognizance of the religious name by putting it on the identity document, but in a different field than the civil name. The facts about a person which determine his or her state identity may change over time. All participants have an interest in keeping this information current. (Schweitzer 2004)

As a matter of legal convenience, the distinction between natural and legal persons was introduced, the latter being organisations of one kind of another having rights and duties of their own and thus needing to be identified so that the right entity enjoys its rights and performs its duties.

The concept of digital identity does not in itself bring with it any really fundamentally new quality not already contained in the state identity. Essentially, it is still just a technique for linking natural or legal persons to a set of known facts about those persons for the purpose of invoking real-world operations on the right persons, i.e. that a certain corporation receives a contract and not another one, or that a given individual shall get or lose a driver's license and not an entirely different person. The main change effected by digital identities is that it becomes increasingly practicable to dissolve the partial identities which have traditionally been administered by a variety of different state agencies by fusing them into one single monolithic data package.

Let us now consider a case in point – *pars pro toto* – the Österreichische Bürgerkarte, or Austrian Citizen's Card.

The citizen's card has been available in Austria since 2003. It enables the use of online services for the identification and authentication of persons, as well as the secure transmission of data. It can also be used for the digital signing of documents. The citizen's card can be used in combination with other cards, such as student IDs, medical insurance cards, bank cards and – unsurprisingly – the Austrian personal identification document. The citizen's card also has the capability of incorporating powers of attorney or procuration, since legal persons also have a need to transact business online and since they are represented by natural persons in doing so. All the different functional facettes attributed to the card-holder are reflected in the so-called ‚citizen's card environment'. This contains the card token (or Smart Card) plus a communication interface for the token for displaying data encoded in the card or for the verification of digital signatures. In other words, the 'environment' is not physically limited to the card itself; the periphery includes external systems, as well.

The card's key certificates are linked to a personal identification number, in order to achieve what is called a "personal bond" between the card and its holder. This ID number serves as a unique identifier; it is generated from the personal ID number held by the Austrian central registry of persons by means of a strong encryption algorithm. For legal persons, the corresponding numbers in the corporate registry or the association registry are used. If a service requires a clear identification of an authorised person, the personal ID number is encrypted uniquely for each transaction, so that the activities of a given person cannot be traced via his or her transactions. The data on the citizen's card are encrypted in a keybox and an infobox respectively. Different access codes can be defined for each type of box. At least two distinct key pairs are stored in the card's key boxes; one is reserved for digital signing, the other is for authentication and encryption. The infoboxes contain further data: the IdentityLink, which handles the 'personal bond' as was mentioned above, and the Mandates, the various things the natural person holding the card is authorised to do. It is also possible to include a link or other reference to an information source external to the card. The suggestion here is that a public trustee or a court-appointed receiver holding a large number of mandates can use the referencing technique to validate them via external databases.

The advocates of the Austrian Citizen's Card like to praise its flexibility and the openness of its technical approach. It is claimed that it can be integrated into a EU-wide or even worldwide ID card system.

Although it is still too soon to be able to say with any certainty whether the Austrian Citizen's Card will become popular and therefore widely accepted in the population, it seems clear that a large variety of attractive features are embodied in it, such as making it possible to claim services online for which a personal appearance in a government office would otherwise have been necessary. Yet data protection specialists have expressed concerns about this project, most recently at the Summer Academy 2005 of the Schleswig-Holstein Data Protection Agency.

Due to its relatively open platform and system architecture and its ability to integrate a wide range of services, the Citizen's Card will probably become quite popular in the long run. Being very expensive, the card-holder, once he or she has acquired the card, has an enormous incentive to load it with as many mandates, i.e. services, as possible. In so doing, he or she will also be increasing his/her transparency with regard to the state apparatus.

5 Conclusions

There is no particular reason why a state's or a government's subjectively felt need not only to authenticate or validate details of peoples' lives, citizenship or other civil status, but also to know practically everything there is to know about them, should rank higher in a rational hierarchy of values than the fundamental human right of privacy.

Data and privacy protection laws in the European Union countries usually show a marked preference for the purported interests of governments over those of individuals. Anyone who has ever filled in a government application form for just about anything in Germany knows that many questions will be posed

in the form, the relevance of which is not immediately obvious. (There may actually be statutory reasons for some of these questions, or they may just stem from the idle curiosity of the civil servants who designed the form. The person making the application usually has absolutely no way to tell the difference.)

Once the required data have been entered in the form, there are of course rules as to which data can lawfully be passed on to which other state agencies – and under what circumstances this will be permitted. As a practical matter, however, the individual involved has no real way of determining whether these rules have been faithfully adhered to. In 1983, the German Constitutional Court stated that the right to "informational self-determination" was a fundamental one. This holding has not, however, led to much in the way of statutory reinforcement. Its principal function is to serve as a guideline for the activities of government officials. There are – it is true – data and privacy protection ombudspersons to whom one may complain if one suspects that one's rights have been violated, but the ombudspersons have no enforcement authority: they may inform themselves about the alleged violation and make recommendations as to possible remedies; and that is all they can do. If the matter goes to adjudication, the ultimate sanction possible by law is that the data which have been wrongfully acquired shall be deleted.

If data and privacy protection laws are to be taken seriously, they must embody some form of deterrent. If a worker in private industry violates a safety regulation, his or her company will be fined and the fine may well be docked from the worker's pay. This type of sanction is the minimum which will actually be effective in practice. The person or persons whose actions directly violate someone's civil rights must be made to pay compensation out of their own pockets. This is the lowest deterrent level. Other civil or labor law sanctions (demotion or dismissal) should be enabled for serious offenses or for repeat offenders. Criminal sanctions should also not be dismissed out of hand. In the U.S., the state of Virginia enacted criminal anti-spam legislation, on the basis of which a notorious spammer was sentenced to nine years in prison and several others have been indicted. Although this might seem rather drastic to some people, particularly since civil recourses against spamming are only a fairly recent development (as, of course, is spamming itself, which was invented in 1994 by a married couple in Arizona), it should be recalled that what is now referred to as "insider trading" was not only perfectly legal within the memory of persons still living, it was actually considered to be a sort of salary additive, a financial incentive to be part of the business world. But behaviors and mores change, while society responds to these changes with new systems of rewards and punishments. There is no reason why violations of data and/or privacy protection laws should not result in criminal sanctions, or why police and prosecutors should not enforce such laws as vigorously as they do other pieces of criminal legislation.

One conclusion (there are, of course, others) to be drawn from these considerations would be that persons not be required to surrender huge amounts of personal information in order to take part in the system. This in itself would vastly reduce the potential for abuse. Surely the state apparatus might reasonably extend the same degree of trust to its citizens that business owners all over the world extend to perfect strangers who offer to pay for an article by credit card. That the occasional card-holder is fraudulent or in default of payment is not perceived as in any way invalidating the utility of the system itself. No one advocates extensive (and cost-ineffective) measures to prevent each and every such occurrence. Rather, these are collateral costs of doing business. The same principle applies to eGovernment and eCitizenship.

References

Dempsey, James X. et al. 2003, *Privacy and E-Government. A Report to the United Nations Department of Economic and Social Affairs as background for the World Public Sector Report*. E-Government Center for Democracy and Technology, Washington.

European Parliament. 1995, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on*

the free movement of such data. [Online] URL:http://www.cdt.org/privacy/eudirective/EU_Directive_.html [last access: 06.12.2005]

Global Internet Policy Initiative. 2004, *THE INTERNATIONAL LEGAL FRAMEWORK FOR DATA PROTECTION AND ITS TRANSPOSITION TO DEVELOPING AND TRANSITIONAL COUNTRIES.* [Online] URL:http://www.internetpolicy.net/privacy/20041228privacy.pdf [last access: 29.11.2005]

International Chamber of Commerce. 2003, *Privacy toolkit. An international business guide for policymakers.* [online] URL: http://www.iccwbo.org/home/e_business/word_documents/TOOLKIT-rev.pdf [last access: 14.12.2005]

Jonas, George. 2004, 'Biometrics won't Catch Disposable Terrorists.' *National Post,* January 19, 2004. [Online reprint] URL: http://www.benadorassociates.com/article/1336. [last access: 10.12.2005]

Organisation for Economic Co-operation and Development. 1980, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. [Online] URL: http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html. [last access: 05.12.2005]

Schmidt, Andréa. 2005, 'Haiti's Biometric Elections: A High-Tech Experiment in Exclusion' *Z Magazine Online,* October 04, 2005. Available from: http://www.zmag.org/content/showarticle.cfm?SectionID=55&ItemID=8865 [last access: 16.12.2005]

Schweitzer, Raffael. 2004, *Globale digitale Identitäten für E-Business und E-Government Ein Realisierungskonzept für digitale Vollmachten* [online]. Effretikon, Switzerland, Diplomarbeit im Fach Informatik, Institut für Informatik der Universität Zürich / 1. Oktober 2004. Available from: URL: http://www.ifi.unizh.ch/egov/Diplom_Schweitzer.pdf [last access: 12.12.2005]

Simpson, Glenn R. 2001, 'Big Brother-in-Law: If the FBI Hopes to Get The Goods on You, It May Ask ChoicePoint'. *Wall St. Journal*, April 13, 2001.

Vartanian, Thomas P. et al. 2002, *21st Century Money, Banking & Commerce* [online]. Available from: http://www.ffhsj.com/21stbook/chapters/ch12intr.htm [last access: 10.12.2005]

Warren, Samuel & Brandeis, Louis. 1890, 'The Right to Privacy'. *4 Harv. L. Rev. 193, 213*

Zweig, Stefan. Die Welt von gestern. Erinnerungen eines Europäers. 34. Auflage, Frankfurt am Main 2003, (first published in 1944) ISBN 3100970470