

# Balancing Security and Privacy in eGovernment Services

Kieran SULLIVAN<sup>1</sup>, Jim CLARKE<sup>2</sup>

Telecommunications Software & Systems Group, Waterford Institute of Technology, West Campus, Carriganore, Waterford, IRELAND

<sup>1</sup>Tel: +353-51-302915, Fax: + +353-51-341100, Email: ksullivan@tssg.org

<sup>2</sup>Tel: +353-71-9166628, Fax: + +353-51-341100, Email: jclarke@tssg.org

**Abstract:** Advances in digital technology are increasing the volume of computer data and accelerating the massive integration of software into our daily lives. The widespread interconnection of networks and digital convergence accentuates this computerization process, making computing, telecommunications and audiovisual information increasingly compatible and interoperable. eGovernment services to citizens and businesses can take advantage of these developments. However, security and privacy concerns must be properly addressed if eGovernment services are to be both fully functional and enjoy significant take-up by end-users. These are not straightforward issues, though, and the resolution of the interplay between security and privacy cannot be achieved by a purely technical means. Instead, there is a balance required between the technological and societal elements; of which there has been significant exploration and reflection recently in the EU Trust and Security communities [1]. In the on-line world, the conflict between privacy and security often manifests itself in a debate between anonymity and accountability. This paper expounds on this apparent dispute by describing the properties of anonymity and accountability; presenting an instructive use case; and, extracting some conclusions with regard to the consequences for relevant stakeholders, should either of these two properties triumph over the other. Steps towards quantifying and measuring the various components that comprise security and privacy are also outlined.

**Keywords:** e-Government services, trust, security, privacy, identity, trustworthy ICT, anonymity, accountability

## 1. Introduction

Continuous electronic miniaturization, the acceleration of communication networks' performance and the inexorable deployment of computing infrastructures is creating a digital urbanization where everything appears closely connected, facilitating inter-communication and access to services and information. Progress in wireless technologies has made possible the popularisation of mobile communication and has substantially changed the way that businesses and Governments operate. The establishment and interoperation of the three complementary ubiquitous environments of *computing* (information stored, processed and presented here and now), *communication* (access anytime, anywhere, using the available best channel) and *storage* (collected, stored, described and displayed information and knowledge, available anywhere, anytime) is gradually surrounding individuals. The value of digital possessions may soon exceed that of material ones, for individuals, businesses and Governments.

Future services will be based on the notion of context and knowledge. They will have to cope with highly dynamic environments and changing resources, and will have to evolve

towards more implicit and more proactive interaction with humans. Security and privacy issues are to the fore of these requirements.

While eGovernment services to citizens and business will bring about considerable cost savings and green computing credentials, adequate security and respect for the end-users' privacy are two non-straightforward key requirements for any eGovernment infrastructure. These are complex issues and both must be addressed holistically, if eGovernment services are to be properly structured and gain the confidence and involvement of end users. Additionally, there must be a strong visual display of these issues being tackled if there is to be significant end-user take-up of such services.

There are many elements that underpin security and privacy. To demonstrate the complexity involved in properly addressing these concepts, this paper examines in some detail two of their underlying elements; namely, the notions of anonymity and accountability. Anonymity and accountability are supposedly opposing factions in a zero-sum game between privacy and security. Conventional wisdom holds that decreasing anonymity (less privacy) is proportional to increasing accountability (more security) [2]. However, as Bruce Schneier [3], states,

“If you set up the false dichotomy, of course people will choose security over privacy -- especially if you scare them first. But it's still a false dichotomy. There is no security without privacy.”

Conversely, this paper looks at the anonymity “versus” accountability debate and asserts that both characteristics can and must exist side-by-side in any on-line environment. Neither concept is enough on its own; nor should any person or business have to choose to avail of only one or the other.

This paper is structured as follows: section 2 provides background information on the concepts of anonymity and accountability, and also highlights some drivers of current security research. Section 3 contains a sample use case which adds real-world context to the security versus privacy debate. A possible solution is offered in section 4, together with a discussion on the concept of personal data. Section 5 describes issues to consider when implementing any solution, as well as a brief examination of the trust aspects which must be addressed in any eGovernment infrastructure. Section 6 draws conclusions from this paper and, finally, Section 7 discusses future work in this area.

## **2. Background**

### *2.1 Anonymity*

Anonymity refers to the absence of identifying information associated with an interaction [4]. On-line interactions can facilitate both more and less anonymity than those carried out in the physical world. Interpersonal transactions across the Internet allow greater anonymity at one level, but there is an identifying data trail left by the Internet user. Such data can include names, dates-of-birth, credit card numbers, mailing addresses and buying patterns.

Research into the provision of on-line anonymity has resulted in the availability of a variety of system designs [5]. While these anonymity systems are effective against several types of attack on privacy, they also result in much slower network performance and cannot protect against more powerful attempts on privacy breaches. Further, such systems are typically overlay networks and, therefore, carry additional overhead costs, since an anonymised connection routed via multiple proxies must pass through several Internet connections before reaching its destination. Reply traffic faces the same overhead. Hence, optimization of this framework is limited.

## 2.2 Accountability

An action is accountable if it can be attributed to someone (or something – such as a service provider – in this context). Accountability on the Internet is made possible by technical attributability. For example, associating a name/identifier to an IP address means that anyone sending malicious content from that location can be traced to that address. This is useful, since a lack of accountability generally means a lack of incentive against bad behaviour. Complete traceability/identification is also undesirable, as the ability to speak freely, without fear of oppression (i.e. anonymously) is a fundamental human right.

To facilitate on-line accountability, two options seem promising and coherent: (1) Base the demand for traceability and accountability on global accountancy-type principles, which can encompass all networks, such that reliable and almost exhaustive incoming and outgoing accounts can be drawn up. (2) Reintroduce, on a lower network layer, a “territorialisation” of data and participating parties [6]. The overall aim is to ensure that people and places can be guaranteed within the current communications system - whose weakness stems precisely from the difficulty in identifying and authenticating these parties - as well as actions in terms of time and place.

By partially moving system control towards establishing data either *a priori* or *a posteriori*, the two approaches outlined can considerably reduce the need for risk-laden recourse to cumbersome identification methods through permanent and intrusive monitoring of all data flows. Other approaches have been suggested and are worth looking at in greater detail; however, the two principal options mentioned above seem to have immediate unifying and organisational potential.

## 2.3 Trends

Current drivers of security and privacy research in eGovernment services include:

- increasing volume of transactions, and even higher volume of traffic;
- increasing mobility of users (physical or virtual), seeking either continuous (mobile) or intermittent (nomadic) connection and access to information and services;
- large growth of sensors and slave-labour devices (*Internet of Things*), taking over the management of routine operations in commerce, utilities, the environment, and law enforcement and security provision;
- convergence of types: voice, visual, entertainment, social and business services. (For example, twitter.gov, and ‘official’ blogs);
- increased, heterogeneous accessibility to converged information and services.

## 3. Use Case

With the above background information in mind, the following scenarios provide additional context for the anonymity “versus” accountability debate:

*Case 1: Alice is a student who puts up an anonymous web site with allegations that the President is a disgrace to the nation because he secretly disfavours a particular nation.*

*Case 2: Alice is a student who puts up an anonymous web site with allegations that the President is a disgrace to the nation because he takes money for allotment of government positions.*

Case 1 is surely worth anonymous protection, but Case 2 seems to add weight to the belief that there should be increased accountability on the Internet.

However, the potential for abuse of power by traceability-seeking governments/administrators is much greater than that of an unidentified “ranting” user.

Further, damage that is produced by an anonymous ranter can be controlled relatively easily by a government/administrator, in comparison to the difficulty which the anonymous ranter would have in trying to control the damage produced by an intrusive government. Thus, the balance between anonymity and accountability should be weighted on the side of the user's anonymity.

This instance implies that the ability to remain anonymous in certain contexts should, therefore, be built into eGovernment services. With such a solid building block in place, the mechanisms to ensure accountability can then be pursued.

#### 4. Two-Tier Internet Solution

The above scenario might be less ambiguous if a secure Internet (accountable) and a “free-for-all” Internet (anonymous) existed simultaneously. In this situation, the student, Alice, could use the appropriate identity – governmental, professional, consumer, whistleblower (anonymised), etc. – when posting her allegations. The weight of Alice's allegations could then be measured against the strength of the identifier she uses when making the claims.

On the secure Internet, the allegations might be taken seriously, as Alice would be required to reveal some identifying information before being allowed to post – thus, she would have opened a channel of redress for the possibly defamed character in her claim. Conversely, on the “free-for-all” Internet, where accountability is limited, the allegations might be akin to someone ranting alone in an empty room or in a room that no authority cares about and to which no one ever pays much heed. Such “free-for-all” forums should not, however, become the equivalent of a sidelined *Speaker's Corner*<sup>1</sup>. To be walled inside a hermetically sealed environment, unable to be heard in the outside world, would not do justice to the rights of the political dissenter, for example.

##### 2.1 Data Ownership

An element which must also be addressed in any viable solution, but which was not explicitly covered in the above use case is that of data ownership. In the EU, the recognised concept is data *controller*, rather than owner. This is a complex issue however, as **Opinion 4/2007** of **Article 29** [7] has shown. Government services and the accessing of same by citizens and businesses have always had a degree of traceability. eGovernment services bring this traceability to new level, especially when the concept of personal data, the use of media recording and virtually unlimited storage capacity are considered.

In 1948 the UN adopted its Universal Declaration of Human Rights (UDHR), which states in Art.12: “*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, not to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*” The 28th International Conference of Data Protection and Privacy Commissioners (London, 2006) stated: “*The protection of citizens' privacy and personal data is vital for any democratic society, on the same level as freedom of the press or the freedom of movement. Privacy and data protection may, in fact, be as precious as the air we breathe: both are invisible, but when they are no longer available, the effects may be equally disastrous.*” In this context, when accessing eGovernment services, great attention must be given to assuring privacy and protection of citizens' data. However, this should not impact negatively on the general public interest; the interests of involved parties; or any legal and contractual obligations.

Protection of personal data is one of the most important aspects of privacy. The person concerned (data subject) would like to be in control of his own personal data or to trust the service provider who handles it. The role, trustworthiness and accountability of the relevant

---

<sup>1</sup> An open area where public speaking is allowed, but the audience size is limited and speaker easily ignored.

data controllers are therefore of crucial importance, since much personal data will be under their control. Technology support in this process is essential, so as to provide the necessary knowledge and tools to the data subject to exercise his/her options, including the ability to act anonymously; and to ensure transparency and accountability of the data controller towards the data subject to enable assessment of trustworthiness.

## 5. Implementation

A strong theme to have emerged from Privacy Enhancing Technology (PET) research over the past few years is that anonymity/accountability properties have to be considered at both the transport (network) layer and application layer. If an anonymity property is not guaranteed at the transport layer, it could prove to be very difficult to “put back in” at the application layer.

There is also the issue of costs involved, when attempting to achieve either anonymity or accountability. This is especially pertinent in cases where the underlying transport layer does not support the respective feature.

If level *n-1* does not support anonymity or unobservability, then these properties become expensive to realize at level *n*. This is due to the need for establishing an anonymity set for every action; i.e. it is a recurring operational expense. This usually makes an activity much more expensive each time. For example, when trying to hide the direction of a message via dummy traffic, many (false) messages have to be sent, as opposed to just the one (true) message.

On the other hand, if accountability is not supported at level *n-1*, it does not seem to be as expensive as anonymity to realize at level *n*. There may well be a high one-time-cost to issue the identifiers needed for accountability. And there may be also some recurring costs involved in maintaining these identifiers, but this is not necessary for every transaction. The effort to “identify” transactions will not be as high as the cost of the respective transaction itself (unlike building an anonymity set, which is more expensive).

### 2.1 Infrastructure and Governance

While multiple technical aspects are important for providing privacy, security and trust, one must recognise that just the technical nuances of security do not automatically imply a “trustworthy system”. A *bona fide* trustworthy system must also entail quantifiable and auditable technical and organisational aspects of delivery (policies, architectures, Service Level Agreements, etc), as well as the user’s perceptions on its operation. When developing eGovernment infrastructures one must consider metrics, certification, standardisation, governance and management, and international agreements on interoperability (including process interaction, definitions and meta-level standardisation and technical interoperability), or federation of often incompatible systems and platforms. Trust requires an infrastructure to build trust relations, using tools to confirm, measure or rate various aspects such as identity, reputation, relationships, risks, or security of the eGovernment environment. It requires instruments to ensure a certain level of transparency and accountability, dependent on the situation.

At the basis of trust lies the assessment of claims from the party to be trusted, be they the eGovernment service provider or the end-user. A basic framework for managing claim verification, including identity, non-repudiation, creditworthiness, reputation etc. is needed to develop federated, open and trustworthy platforms in various application sectors. Electronic Identity Management (eIdM) systems are available, integrated in services provided by industry or by public administrations. However, interoperability is practically non-existent, nor is sufficient attention given to privacy and minimisation of data exchange.

Banks, for example, mostly have their own ID systems, but these have no connection to citizen registrations other than via an ID card or passport.

## 5.2 Global Solutions

International cooperation efforts in the areas of trust, security, privacy and identity management should be studied – when considering interoperability issues, in particular – since solutions that are globally relevant will have the greatest impact. The INCO-Trust project [8], for example, has established a framework for collaboration between European Union program managers and research communities within ‘Trustworthy ICT’ and countries including USA, Japan, Australia, South Korea and Canada. Broadening this initiative to include other nations, including Africa, would further synergise the work already being done on the various aspects that comprise trustworthiness and secure, privacy-respecting services.

## 6. Conclusions

Current research indicates that anonymity is expensive to realize if the underlying network/transport layer does not have unobservability built in. Conversely, accountability is relatively easy and inexpensive to achieve if the underlying layer does not support anonymity. Thus, it may not be advisable to primarily focus on achieving accountability and then proceed to level everything down to achieve anonymity/unobservability; the other way around may prove to be more fruitful. It should be remembered too that just because accountability at the transport layer means that anonymity is nearly impossible at the application layer today does not mean that this will be the case in the future.

What also needs consideration is the concept of non-binary anonymity; which is likely to be more prevalent in citizens and businesses accessing eGovernment services. Localised transparency/accountability (i.e. in a specific context) can lead to “graded” anonymity; thereby, increasing privacy outside of the local/specific environment.

Finally, it is worth recalling that the promises and guarantees given by service providers with regard to the confidentiality of users’ data are only as worthwhile as the governing authorities allow. If a future administration hinders such privacy, then today’s industry may well require systems for untraceable communications. This does not mean that everybody should be allowed to carry out transactions anonymously, but it does support the point for essentially anonymous communication infrastructures, on which one can build traceability.

This paper has demonstrated the complexity of the various concepts that comprise security, privacy, trust and identity in ICT environments. It has also described some of the issues to be considered during the deployment of trustworthy eGovernment services, as well as pointing towards some possible solutions to the task at hand. If eGovernment services to citizens and business are to be successful and enjoy consumer confidence and user up-take, then the providers of such services should be aware of each of these interconnected elements of trustworthy service provision.

## 7. Future Work

While the literal meaning of anonymity, accountability, responsibility, transparency, authentication, unobservability, measurability and others may be well understood, their relation to each other in the context of providing secure eGovernment services may not always be so obvious.

To address this uncertainty, future work by the authors will begin the process of mapping and interlinking glossary terms from the current ICT security and privacy domain. It is anticipated that such a high-level graphical tool will contribute directly to the knowledge of the specific attributes involved and also, therefore, to the overall

understanding of security and privacy in the context of eGovernment services. To achieve this goal, the authors propose designing an ontology-based tool that will capture and relay the appropriate vocabulary in an illustrative and straightforward manner [9, 10].

A *trust-terms* ontology would be appropriately codified in order to make it machine-readable for the different software agents across the implementation layers of eGovernment services. The various stakeholders involved in the provision and consumption of these services could use the *trust-terms* ontology to formalize the security and privacy requirements of their own particular domain. The ontology would also serve as a basis to produce a glossary to suit the needs of specific groups of stakeholders. This would be done by inserting additional data into the system via the importation of other ontologies into the *trust-terms* ontology; thereby reusing existing knowledge and information. Once the eGovernment services identify their security and privacy requirements, the weighting of the various attributes, to reflect their relative importance in different domains, would also be a natural step forward.

## References

- [1] Think-Trust EU-IST FP7 Coordination Action Project (2009) 'Trust in the Information Society: RISEPTIS Report', available: <http://www.think-trust.eu/riseptis.html> [accessed 29 Oct. 2009].
- [2] Gorman, S. (2008) 'Dancing Spychief Wants to Tap Into Cyberspace', *The Wall Street Journal*, available: <http://blogs.wsj.com/washwire/2008/01/13/dancing-spychief-wants-to-tap-into-cyberspace/> [accessed 16 Oct. 2009].
- [3] Schneier, B. (2008) 'Security vs. Privacy', *Schneier on Security: A blog covering security and security technology*, available: [http://www.schneier.com/blog/archives/2008/01/security\\_vs\\_pri.html](http://www.schneier.com/blog/archives/2008/01/security_vs_pri.html) [access 23 May 2009].
- [4] Nissenbaum, H. (1999) 'The meaning of anonymity in an information age', *Information Society* (15), p. 141–144.
- [5] Dingledine, R., Mathewson, N. & Syverson, P. (2004) 'Tor: The next-generation onion router', *Proceedings of 13th USENIX Security Symposium*, San Diego, California, USA, 6-9 Aug: USENIX Association.
- [6] Think-Trust EU-IST FP7 Coordination Action Project (2009) 'Deliverable D3.1-A Recommendations Report (Interim)'
- [7] Council Directive (EC) 1995/46/EC of 20 June 2007 'Opinion 4/2007 on the concept of personal data'.
- [8] INCO-Trust EU-IST FP7 Coordination Action Project (2009), available: <http://www.inco-trust.eu/>.
- [9] Blanco, C., Lasheras, J., Valencia-García, R., Fernández-Medina, E., Toval, A. & Piattini, M. (2008) 'A Systematic Review and Comparison of Security Ontologies', in *Proceedings of the Third International Conference on Availability, Reliability and Security*, IEEE Computer Society, Washington, DC, 813-820.
- [10] Viljanen, L. (2005) 'Towards an Ontology of Trust', in *Proceedings of the 2nd International Conference on Trust, Privacy and Security in Digital Business (TrustBus'05)*, Copenhagen, Denmark: Springer-Verlag, LNCS 3592/2005.