LEVERAGING THE POSTAL INFRASTRUCTURE FOR THE AUTHENTICATION OF INDIVIDUALS TOWARDS AN ONLINE GOVERNMENT SERVICE PROVISION

Caroline Sheedy and Maria Moloney*

1. INTRODUCTION

The postal system provides a natural platform for transaction enabling, both in a traditional physical sense and, as we will argue in this chapter, in a digital sense. The existing legal protections offered by the postal system to their customers provide an infrastructure, which if extended into the digital world could provide a secure platform for public eservices transactions. The success of National Postal Operators (NPOs) providing such a digital public service platform in an effective and secure manner depends on their ability to demonstrate appropriate authentication and verification mechanisms to ensure customers' correct identity is consistently established.

Notions of identity and authentication are fundamental concepts in every marketplace. People and institutions usually need to get to know one another before conducting business. Traditional commerce relies on physical credentials, such as a business license or letter of credit to prove their identities and assure the other party of their validity to engage in a transaction. In online environments providing such credentials is somewhat more challenging. This arises from the lack of physical presence of participants involved in a transaction.

Authentication mechanisms are closely linked to the value of what they protect. For example, many people are comfortable with a username/password authentication for their email. For higher value services, such as an online revenue service, an out-of-band[1] mechanism is often employed for multifactor authentication. Authentication is core to achieving a trusted system as it decreases the likelihood of fraud occurring within that system (Parker & Alstyne, 2012).

Given the level of trust individuals have expressed traditionally for the postal service (The Ponemon Institute, 2010), extending the offering of the postal services into the digital domain seems natural. The economic benefits of moving to electronic delivery for governments and centralized services have been examined (US Postal Service Office of the Inspector General, 2013). What has been less considered is the means by which USPS can provide governments for authenticating their citizens. NPOs can provide an existing physical infrastructure, which could be used as an extra layer of physical authentication for citizens when transacting electronically. NPOs could combine this extra layer of authentication with existing digital methods of authentication to provide citizens with a digital identity that they can then use to access public eservices.

Section 2 examines whether NPOs are a natural host for the provision of a digital identity, by examining multifactor authentication mechanisms available to them. It identifies the unique advantages NPOs have over other potential service providers of public eservices. Section 3 then considers the challenges that NPOs would need to overcome should they embrace this role of gatekeeper for public eservices provision. Section 4 reports the results of a survey conducted among members of the public, which sought opinions on whether NPOs are well placed to provide such digital identification. Public opinion is generally supportive of such a move but some concerns persist surrounding the security of

* Escher Group (IRL) Ltd Dublin,

digital identification regardless of the service provider. Section 5 concludes.

2. CHALLENGES AND OPPORTUNITIES FOR NPOs

Currently, NPOs in many countries remain either state-owned companies or independent agencies of the government. In the UK, the Royal Mail is state-owned and La Poste in France and the US postal service are independent governmental agencies. Other NPOs have been privatized, such as Deutsche Post. Regardless of whether publicly or privately run, many NPOs are already tackling the challenge of digitalizing their offerings. La Poste in France has introduced electronic services and offers webmail services to their customers. There has been rapid growth in postal eservices in recent years with 85 electronic postal services of this kind having been introduced globally in 2010 alone, compared to 33 in 2007 (UN News Centre, 2013).

Privatization and the influence of information and communication technologies (ICTs) are changing NPOs considerably. The challenge faced by NPOs now is no longer an issue of whether they should digitalize their service offerings; it is an issue of how best to digitalize them. One appropriate solution for digitalizing NPOs would be to blend their current provision of valued universal services with new forms of digitalized universal services (Moloney, 2013).

NPOs are particularly well placed to become key players in the field of electronic delivery because they are traditionally regarded as Trusted Intermediaries (TIs). They have a responsibility to satisfy the Universal Service Obligation (USO). De Reuck and Joseph (De Reuck & Joseph, 1999) argue that the concept of a USO is relative to the historical moment in which the USO occurs. That is to say, it is not a rigid concept but rather a dynamic one, which requires continual revisiting in light of changing technological innovations and social needs. For example, in Great Britain, the provision of broadband services to all households in the country has recently become a universal service. An NPO's USO could be extended to encompass eservices, or redefined as a Universal *eService* Obligation (UeSO).

Research has shown that given the often profit driven and competitive nature of our digital society and individuals' concerns surrounding issues like the protection of their personal information online, individuals prefer to entrust their personal information to familiar and trusted brands (Shankar et al., 2002). When individuals 'trust' an online brand, it increases the likelihood of those individuals actually interacting with that brand because trust alleviates concerns regarding possible negative consequences (Kim & Prabhakar, 2000). Research has shown that transparency and openness are essential characteristics of trust (Barber, 1983; Covello, 1992; Mishra, 1996; Peters et al., 1997). The next subsection demonstrates how NPOs have been providing open and transparent postal services for centuries.

2.1 The NPO as an Open Communications Provider for the Government

Open systems promote growth (The Berkman Centre for Internet and Society, 2012). This has been demonstrated by the postal system for centuries. Open systems continuously engage with and are informed by their environment. Using open standards facilitates the growth of heterogeneous ecosystems, which evolve to best suit the needs of the users of the system. This makes open ecosystems possible, driving interoperability, sustainability and choice. Open systems help incorporate modularity, portability and scalability while lowering costs. The Berkman Centre for Internet and Society at the Harvard School of Law (2012) has set out five guiding principles for open ICT ecosystems. These principles can easily be applied to the current postal ecosystem, providing support for the argument that the postal system was the original open system.

Interoperable – the postal system has allowed for exchange, reuse, interchangeability and interpretation of information across the globe for over a century now.

User centric – the main function of the postal service is to provide services and mail transfer and delivery to citizens regardless of their location, or perceived location constraints.

Collaborative – One of the main functions of the postal system, since its inception, has been to facilitate the global communication of governments, businesses and citizens.

Sustainable – the postal service ecosystem has evolved and for the most part thrived for over a century.

Flexible – for the best part of its existence the postal system has managed to adapt to changes, this is why it has endured for so long. Now that it is faced with a disruptive innovation, ICT, it needs to revise its business model and become more adaptable to the digital world.

Currently, in countries across the globe, many NPOs and governments work together to use the large number of national postal outlets as delivery points for government services. Naturally, there are differences in terms of the historical, cultural and socioeconomic contexts of national and local government across countries, and there is no universal approach by government bodies for collaborating with the postal service in delivering government services. Nevertheless, citizens worldwide are increasingly seeking ways to access products and services whenever, wherever they want and in ways they find appropriate and convenient. The availability of postal outlets in most towns and villages across a country makes them a logical point of contact for governmental services provision (Triangle Management Services Limited, 2011). In addition, many government agencies across the globe are experiencing budget constraints and resource reductions. Many of these agencies have expensive field office network structures that are often inaccessible to many citizens. Because of the extensive national network offered by the national postal service, government agencies can cut the cost of their existing field office networks by providing their government services through local post offices.

A recent study conducted for Consumer Focus Scotland (Triangle Management Services Limited, 2011) found that a key factor for success in the delivery of any public eservice through the postal system lies in providing the postal staff and licensees responsible for the front line service with the knowledge and skills to deliver accurate, timely products and services. Ongoing training, responsiveness to change and maintenance of service quality are vital to customers and the service owners, i.e. the government.

Learning about interacting with government electronically can be a daunting task especially for those not familiar with ICTs, however, when the training is provided in a familiar setting with well known postal workers, the perceived difficulty of the task can be greatly reduced. Provision of governmental services has been in many countries and could continue to be for many NPOs a viable source of revenue, with minimal setup costs for either party, the government or the postal service (Triangle Management Services Limited, 2011).

3. CONSIDERATIONS FOR POSTAL DIGITAL IDENTIFICATION

As in the physical world, identity in the digital world is context-specific. A digital identity is linked to the actions we perform when authenticated by the model. Some of the most popular of these digital activities include: email (communication), financial transactions and social networks. Increasingly, individuals use multiple devices to access accounts associated with these services, with the average currently being two devices (Bleau, 2013).

Motivating individuals to be cautious regarding the use of specific *subsets* of their digital identity, i.e. their financial identity, is straightforward. The consequences of a compromise of this identity subset are immediate and understood. While the individual's financial institution will reimburse them eventually, individuals are very often still cautious in their use of credit cards. The *breadth* of an individual's financial identity may be less clear, as it does not just include financial information such as bank details but also details such as the individual's pension entitlements, social welfare standing, and even their annual medical expenses.

Another subset of an individual's digital identity is their *communication* identity, which is often linked to their email and social networking accounts. Most people use this identity subset to receive updates on utility bills, social or personal interests, and/or financial statements. A merge of an individual's financial and communication identity subsets could form the basis of an *online shopping* identity, which can be used for buying shoes online or subscribing to a group discount website. Regardless of how the online shopping identity subset is used, the data it contains about an individual reveal how they spend a lot of their time online and arguably offline also. Thus, these identity subsets require some form of access control mechanism, based on an authentication mechanism to ensure an individual's personal data is not compromised or abused.

3.1 Postal Digital Identity

Authentication plays a key role in any digital system. It is well established, and an ongoing trend, that the easiest way to bypass a systems security, while remaining undetected, is to compromise credentials (Verizon.com, 2013).

There are three generally accepted approaches for authenticating the identity of a user. Something the user knows, such as a password; something the user has, such as a physical or otherwise token; and something the user is, such as a fingerprint or voice pattern. In order to use these characteristics to verify the identity of an individual, computer systems use software, hardware, or a combination of both.

Multifactor authentication is increasingly used in practice. This consists of a minimum of two of the following authentication approaches: password-based authentication, token-based authentication and/or challenge response authentication. While the individual components retain their existing properties, e.g., a well chosen complex password is more difficult to crack than a poorly chosen simple one; the merging of at least two approaches increases the difficulty of compromising the security system for an attacker (Verizon, 2013).

One postal digital identity method involves a user, when signing up for the digital identity program from the NPO, being prompted for a username and password that needs to be of a certain length and complexity. In addition to this, a pin code is sent to the user's mailing address. Upon receipt of this pin, the user can log in to the digital identity system (this type of authentication is token based authentication). After initial log in to the identity system, the user will be presented with a challenge response verification process (challenge response authentication). The user must either download a software application provided by the NPO to their mobile phone, or receive a physical device in the postal mail that generates a random number. The user then needs to input a randomly generated number from that device into the digital identity system to access the system (challenge response authentication).

3.2 Postal Digital Identification and Data Protection Legislation

As well as the existence of authentication mechanisms for ensuring digital identity, a series of legal protections exist which safeguard individuals' rights regarding their personal information once submitted in electronic format. Some jurisdictions have stronger data protection legislation than others. The European Union have for some time been known to be more restrictive in their view of permissions surrounding access to their citizens' personal information than has the United States (Rule, 2007).

The European Union Data Protection Directive of 1995 was established to provide a regulatory framework to guarantee secure and free movement of personal data across the national borders of the EU member countries, in addition to setting a baseline of security around personal information wherever it is stored, transmitted or processed (The European Commission, 1995).

The personal data that the Directive covers includes information relating to 'an identifiable person'. This includes information about a natural person directly identified by an identification number or

indirectly with one or more facts that relate to his 'physical, physiological, mental, economic, cultural, or social identity'. Sensitive data is an important subset of personal data. Sensitive data is that which reveals racial or ethnic origin, political opinions, religious beliefs, trade union membership, health or sex life details. This information is regarded as sensitive because it could expose the data subject to discrimination as well as infringe on the very fundamentals of privacy. Health information as defined by this article would include past or present information on physical or mental state as well as any abuse of drugs or alcohol (Herold, 2002).

The Directive on Privacy and Electronic Communications 2002 is an EU directive on data protection and privacy in the digital age (The European Commission, 2002). It builds on the Data Protection Directive of 1995 and applies to all matters which are not specifically covered by the Data Protection Directive. It deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies. Since its enactment, it has also been amended by Directive 2009/136, which introduces changes specifically concerning cookies and unsolicited email or other messages (The European Commission, 2009).

The EU Data Protection directive mandates that the personal data of consumers and employees cannot be transferred by multinationals operating in the EU to their home country unless that country has adequate data protection regulations in place. Historically, the US has been less comprehensive with regard to regulating private sector use of personal information (Rule, 2007). As a result, the European Commission came to an agreement with the US government to ensure continued trade between the two countries. The agreement was called Safe Harbor. It provides a privacy compliance framework and a way for US organizations to avoid experiencing interruptions in their business dealings with the EU, or facing prosecution by the European authorities under European privacy laws. Certifying a US organization to the Safe Harbor requirements was intended to assure EU entities know that the organization provides "adequate" privacy protection as required by the EU Directive. It was intended that the Safe Harbor framework would provide a simpler and cheaper means of complying with the privacy adequacy requirements of the EU Directive, and would also significantly benefit small and medium organizations.

Because Safe Harbor permits American corporations to self-certify the practices that they follow regarding personal information, most organizations importing personal information into the US from Europe frequently disregard the measure (Rule, 2007). As a result of this unequal and complex environment regarding the submission of personal information online, information privacy concerns continue to be evident among users of ICTs (Antón et al., 2010).

In former times, citizens of most countries across the globe, including the US and Europe, enjoyed the protection of their personal information when in transit through the use of their national postal system and beyond through established International postal agreements. NPOs were obliged by law to protect the mail and ensure it arrived at its destination tamper-free. Within many jurisdictions, mail tampering is a crime and is punishable by incarceration, fines, or a term of probation. Within the US, tampering with the mail is a crime under most state laws and mail fraud is a federal crime. The exact definition of mail tampering generally includes opening, destroying, damaging, or interfering with mail intended for another person (USPS.com, 2012). In most countries of Europe it is an offense to open, destroy, hide or delay any post that is addressed to someone else (Campbell, 2008). However, protecting personal information in a digital environment, even with established data protection laws, remains less transparent than in the physical world and unlawful access to citizens' personal information, even at the highest level of government, continue to be reported in the media (Rosenbaum, 2013). The recent reports in the media about how Edward Snowden, a former technical contractor for the United States National Security Agency (NSA) and a former employee of the Central Intelligence Agency (CIA), leaked details of several top-secret U.S. and British government mass surveillance programs to the press (Gellman & Markon, 2013). A significant part of these surveillance programs entailed the monitoring and collection of email communications (Greenwald & Ackerman, 2013). The next section looks at the possibility of NPOs providing a multifactor authentication infrastructure which could form the basis of a digital identity that

NPOs could use to authenticate citizens for accessing public eservices and to prevent the unauthorized access to personal information that is at the heart of these privacy breaches highlighted by the media.

4. THE IMPLICATIONS OF A POSTAL DIGITAL IDENTITY

One of the advantages unique to using an NPO to construct and maintain a digital identity is the preexisting international agreements in place under the Universal Postal Union (UPU). The UPU is a specialized agency of the United Nations that coordinates the worldwide postal system and postal policies among member nations. As a result, there is already an established political infrastructure and a series of international agreements on the safe transfer of information via postal networks across the globe (Universal Postal Union, 2011). These agreements could potentially be revised to include the transfer of information through *electronic* postal networks across the globe. The safe and secure transfer of communications globally has traditionally been the responsibility of the postal service. Extending this duty into the digital world could be seen as simply extending NPOs universal service obligation to the digital domain. Other large organizations which facilitate the transfer of communication through their digital services, i.e. Google, Microsoft and/or IBM do not have the same responsibility to ensure *private and secure* transfer of communications because they are not bound by a universal service obligation and postal legislation like NPOs. Thus, if the UPU's international agreements for the safe transfer of communications were extend to encompass *electronic* communication, NPOs, through International law, would need to provide the same privacy protections for electronic mail as they currently provide for physical mail through the postal system.

However, such a revision would have to ensure compliance of the NPOs with the data protection legislation that has been established in select regions globally to protect the personal data of individuals. This consideration of data protection legislation could be quite complex given the fact that the legislation differs from country to country. Even within the EU, the data protection directives have been interpreted differently in each member state.

Currently, NPOs have no legal obligation to ensure the appropriate handling of personal information or indeed the appropriate managing of digital identities. Thus, the data that would be collected and used by the NPO would need to be treated in a standardized and an agreed upon manner to ensure the data management methods remain transparent to users. For instance, the use of the Royal Mail's Postal Address File (PAF) in the UK[2] or what is called the Geo-directory in Ireland (Geodirectory.ie, 2013), would be advantageous if it could be used as part of a multifactor authentication process for postal digital identification. However, investigations need to be carried out to ascertain whether the use of this file is possible under the data protection legislation of the UK. The following subsection describes a series of focus groups that were carried out to ascertain public opinion on a postal digital identity for the provision of public eservices.

4.1 Discussion on the Attitudes of Individuals towards Postal Digital Identity

In order to understand user perspectives on having NPOs provide digital identification for the provision of public services, eight focus groups each consisting of eight people were set up. They were carried out in both rural and urban settings at two locations in Ireland, namely the west and east of Ireland. Participants of the focus groups were selected from a mailing list of a professional research company. Gender, age and socioeconomic status were considered when making the selection. People with and without personal computers were included, unemployed people and stay-at-home mothers also formed part of the list of participants. Each focus group lasted 90 minutes. The table below describes the demographics of the focus group participants in detail.

Table 2 The demographics of the focus group participant

Group	Age	Knowledge of Computers		Gender	Location
		Standard skills*	Advanced skills†		
1	18-24	50%	50%	50/50 M-F	Region 1
2	25-34	50%	50%	50/50 M-F	Region 2
3	35-44	50%	50%	50/50 M-F	Region 1
4	45-54	50%	50%	50/50 M-F	Region 2
5	55+	50%	50%	50/50 M-F	Region 1
6	18 - 34	50%	50%	50/50 M-F	Rural reg. 1
7	35-54	50%	50%	50/50 M-F	Rural reg. 2
8	18-54	75%	up to 25%	50/50 M-F	Region 1

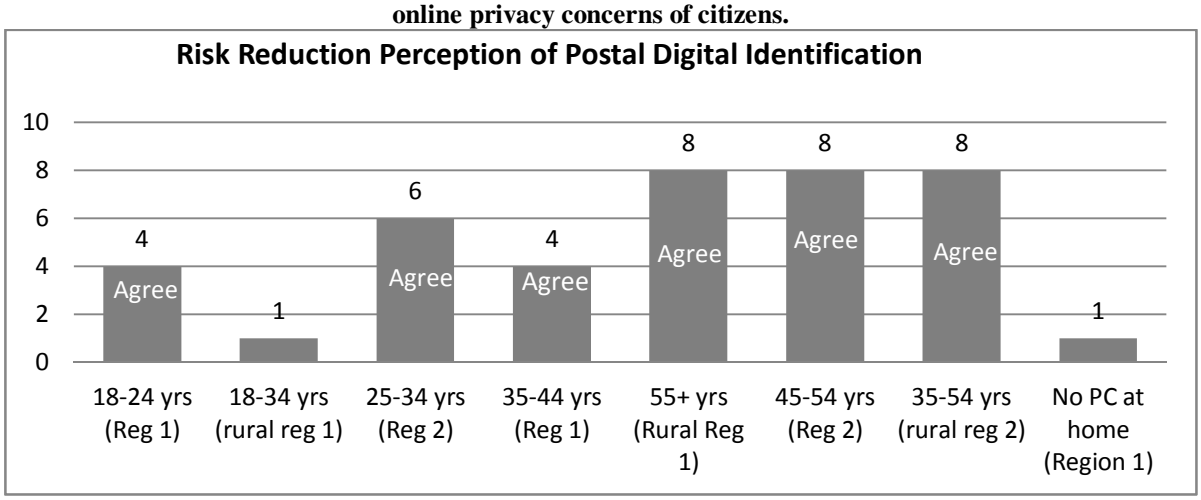
*Participants with standard knowledge of computers were capable of sending email and surfing the Internet for information and entertainment purposes. They had a Facebook and/or LinkedIn account.
†Participants with advanced knowledge of computers were capable of carrying out online banking, shopping, filing of taxes, and e-bill payment.

As a warm up exercise, each participant was asked a set of questions concerning the benefits and drawbacks of the Internet, their main activities on the Internet and their attitudes to online privacy especially when interacting online with government, private companies and public private partnerships. They were then asked to give their opinion on two statements. The first of which was the following:

The provision of a Postal Digital Identity will facilitate public eservices provision by reducing the online privacy concerns of citizens.

The graph below gives a snapshot of the focus groups' acceptance of postal digital identification in terms of the participants' perception of whether it reduces the risk of invasion of informational privacy. Age had the most impact on the acceptance of postal digital identification, which is apparent from the graph. The older generation perceived that the identification scheme had potential to reduce risk when transacting and interacting electronically with their government. There were no differences in this regard between participants who lived in a rural setting and those who lived in an urban setting. The vertical axis of the graph shows how many individuals in each focus group perceived that a postal digital identification scheme would reduce the risk of privacy breach. The horizontal axis shows the eight focus groups and the ages and location of the participants.

Figure 1. The provision of a postal digital identity will facilitate public eservices provision by reducing the online privacy concerns of citizens.



The mature participants of the focus groups (45 years +) who frequently used the Internet understood how finding solutions to online privacy concerns, i.e. authenticated access to personal information reducing unauthorized use of personal information, would be beneficial to them. However the mature participants who infrequently used the Internet did not see any added *personal* benefit to resolving such a challenge. That is to say that some of these participants may have accepted that a postal digital identity would reduce informational privacy concerns but that such a scheme would have no or little benefit for them as they saw a limited need for it in their own lives.

Conversely, some of the less mature participants (<45 years) went as far as to say online privacy was not a challenge but simply an ideal and thus practically impossible to achieve. The majority of individuals who owned or worked in businesses that frequently used the Internet, however, saw a huge benefit to resolving this issue and generally believed their business would benefit from a reduction in the informational privacy concerns of their customers.

In the majority of the focus groups private companies were perceived as an equal or greater threat to individuals' informational privacy as government or public private partnerships. Even though a large portion of the participants were skeptical about their personal information being appropriately used online, they were more inclined to believe that government and public private partnerships had more of a responsibility to safeguard their personal information. These findings are supported by several peer reviewed studies which also found that a stronger threat to privacy, in the past, has come from the private sector rather than from the public sector (Dinev et al., 2008). It was also found that the private sector, rather than the public sector, has been attributed with making consumers, as distinct from citizens, vulnerable. A report from the European Commission found evidence that supported this argument, the public sector is using a variety of approaches to effectively cooperate with data controllers to increase the deployment of privacy enhancing technologies (PETs) (London Economics, 2010). Based on this finding, we argue that NPOs becoming the guardians of citizens' digital identity can reduce the informational privacy concerns of individuals when availing of public eservices from their government.

The finding of the focus groups that individuals prefer to entrust their personal information to public private partnerships is supported by the findings of the Ponemon Institute (Accenture, 2009) in the United States. The Institute conducts an annual survey to assess how citizens perceive government agencies' ability to handle the challenge of keeping personal information private. Ponemon surveys 9,000 consumers regarding 75 federal agencies annually. In 2010, the overall average approval rating for trust of government agencies dropped from 50% in 2009 to 38%. However, more than 87% of the 9,000 Americans surveyed ranked the US Postal Service (USPS) as the most trustworthy government agency among all 75 agencies. It was the sixth year running that the USPS had won this award. Ranking as the most trustworthy government agency indicates that Americans trust USPS to keep their information safe and secure (Teinowitz, 2011).

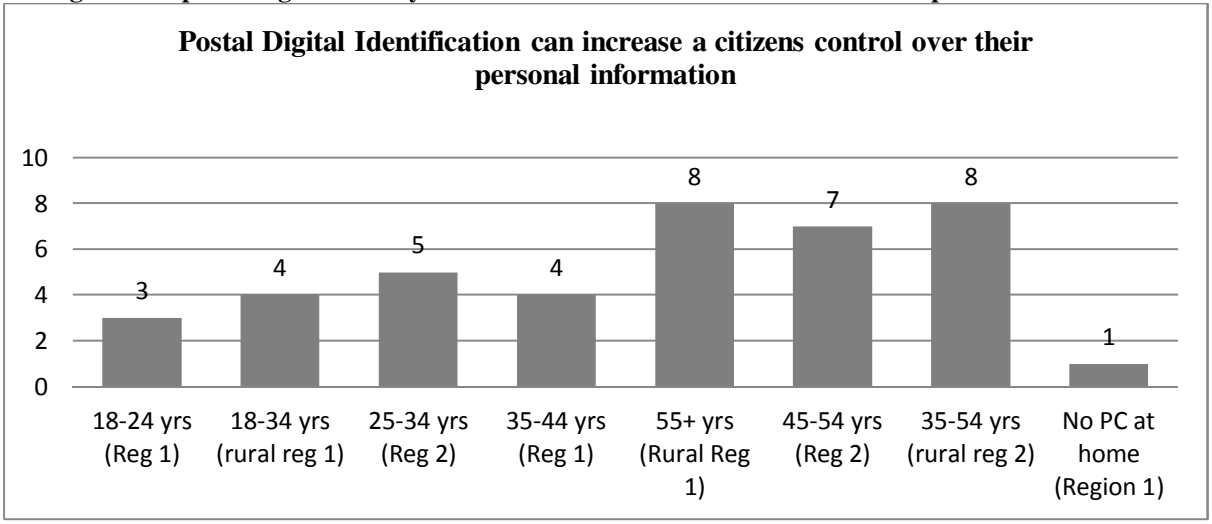
A significant finding, however, was that participants had reservations about the technical competencies of public bodies to safeguard private information. The majority of participants believed that private companies like Microsoft, Google and IBM had far superior technical expertise and financial resources to invest in research and development in how to safeguard personal data stored within their systems. These findings are similar to the findings of Kim and Prabhakar (2004) who found that trust in the actual technology that provides a service is an important determinant of IT adoption. A view that is echoed by Kelly et al. (2002) who, when analyzing what it is that citizens value in respect to government and public services, identify three categories, (1) positive personal experience of public services, (2) positive perceptions of service outcomes i.e. how much public value is created by the service, and (3) trust. They also argue that a failure of trust destroys public value. Grimsley et al. (2003) demonstrate a positive correlation between satisfaction with public services and trust in public services.

The second statement that the focus group participants were asked to give their opinion on was the following:

A postal digital identity has the potential to redefine/transform the USO by giving more control to citizens over their personal information

The above statement was put to each of the focus groups and their opinions were sought in response. The notion of control was debated from two perspectives: 1) control over whether to submit personal information online or not, and 2) control over personal information once it is submitted. The majority of participants agreed that a postal digital identity increased user control once their personal information was submitted online and as a result, it satisfied one aspect of user control (Figure 2). This increase in control over submitted information was seen as a benefit of a postal digital identity and the majority of the participants were prepared to interact with their government with such a scheme.

Figure 2. A postal digital identity would increase a citizen's control over their personal information



However, the majority of participants had general reservations about submitting their personal information electronically. With regard to controlling the submission of sensitive information online, participants felt such a postal digital identity did not increase their perception of control, in fact many felt it would put more pressure on them to interact with their government electronically. The participants that had no PC at home were particularly sensitive to this issue arguing it would involve a substantial change in their habits to adopt this method of interacting with government as they would probably have to invest in a home computer.

Age had an impact on how much participants believed the method would increase their control over their personal information. The older the participant, the greater the increase in control over personal information the participant perceived to get from having a postal digital identity. Some of the younger age group participants were not impressed with the claim that it would protect the informational privacy of citizens, arguing that identity schemes existed already and they (the participants) were more than adept at protecting themselves online without the help of post offices or the government.

Initially the majority of participants accepted the postal service as a trusted authority. The postal service was viewed as trusted, community oriented, maybe a bit antiquated, but benign, non-threatening and experienced in communication delivery. When the majority of participants were informed that the postal service would administer postal digital identification NPOs came under heavy criticism, from a technical point of view, for their capability and expertise. The majority of such criticism came from the younger participants. Their capabilities were compared with IT giants like Google and IBM and it was agreed they were very much at a disadvantage in terms of their capabilities for ensuring the authentication system behind the postal digital identity would be secure against a security or privacy breach.

The findings of the focus groups suggest there is still a feeling among the public that NPOs still have a role to play in providing secure communications and that this could extend to the digital world, once certain issues are addressed. For example, NPOs would need to employ the expertise of established software development and security organizations to increase citizen trust in their ability to appropriately implement and maintain the technology needed to provide a digital identity scheme. NPOs trusted brand as a benign, community oriented communications provider seems to have endured. However, its ability to successfully transform this brand for the digital world remains to be seen.

5. CONCLUSION

This chapter evaluated the notion of using the existing postal infrastructure to provide a stronger form of online authentication through combining physical address verification with online authentication to form a postal digital identity that could be used to facilitate access to public eservices. It considered the benefits of using an already established universal open system, the postal system, to continue to transfer personal information around the globe privately and securely as it has done for centuries but in digital format instead of traditional physical mail format. It identifies the benefits of using NPOs as the administrators of such a system because they could combine both physical authentication with digital authentication to provide multifactor authentication for increased security when interacting electronically with government and when submitting personal data online.

Additionally, the chapter examined the issues that need to be considered if such an authentication scheme were introduced. In particular, it looked at the complexity of the diverse data protection laws of both the EU and the US and their potential impact on this postal digital identity if deployed. It also looked at the attitudes of individuals that took part in a series of focus groups to understand their opinions on whether postal digital identification would help to reduce informational privacy concerns. The preliminary responses from the participants were generally positive.

6. REFERENCES

Accenture, 2009. *How Global Organisations Approach the Challenge of Protecting Personal Data.* Accenture.

Antón, A.I., Earp, J.B. & Young, J.D., 2010. How Internet Users' Privacy Concerns Have Evolved Since 2002. *IEEE Security & Privacy*, vol 8((1)), pp.pp 21 - 27.

Barber, B., 1983. *The Logic and Limits of Trust*. New Brunswick, New Jersey: Rutgers University Press.

Bleau, H., 2013. *RSA Speaking of Security. Digital Identities: I Have One For Sale*. [Online] Available at: https://blogs.rsa.com/digital-identities-i-have-one-for-sale/ [Accessed 29th April 2013].

Campbell, D., 2008. International Telecommunications Law, 2008., 2008. Yorkhill Law Publishing.

Covello, V.T., 1992. Trust and Credibility in Risk Communication. *Health Environment Digest*, 6(1), pp.1-4.

De Reuck, J. & Joseph, R., 1999. Universal Service in a Participatory Democracy: A Perspective from Australia. *Government Information Quarterly*, Volume 16(Issue 4), pp.Pages 345-352.

Dinev, T., Hart, P. & Mullen, M.R., 2008. Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *Journal of Strategic Information Systems*, 17, p. 214–233.

Gellman, B. & Markon, J., 2013. *The Washington Post. Edward Snowden says motive behind leaks was to*

expose 'surveillance state'. [Online] Available at: http://www.washingtonpost.com/politics/edward-snowden-says-motive-behind-leaks-was-to-expose-surveillance-state/2013/06/09/aa3f0804-d13b-11e2-a73e-826d299ff459_story.html?tid=pm_politics_pop [Accessed 8 July 2013].

Geodirectory.ie, 2013. *Every single address at your fingertips*. [Online] Available at: http://www.geodirectory.ie/ [Accessed 29th April 2013].

Greenwald, G. & Ackerman, S., 2013. *The Guardian. NSA collected US email records in bulk for more than two years under Obama*. [Online] Available at: http://www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama [Accessed 8 July 2013].

Grimsley, M., Meehan, A., Green, G. & Stafford, B., 2003. Social Capital, Community Trust, and E-government Services. In *The First International Conference on Trust Management, iTrust*. Heraklion, Greece, 2003. available at: http://link.springer.com/chapter/10.1007%2F3-540-44875-6_12.

Herold, R., 2002. European Union (EU) Data Protection Directive of 1995: Frequently Asked Questions. *Computer Security Institute (www.gocsi.com)*.

Kelly, G., Mulgan, G. & Muers, S., 2002. *Creating Public Value. An Analytical Framework for Public Service Reform.* [Online] The Strategy Unit, UK Cabinet Office Available at: http://www.cabinetoffice.gov.uk/strategy/seminars/public_value.aspx [Accessed Nov 2009].

Kim, K. & Prabhakar, B., 2000. Initial Trust, Perceived Risk, and the Adoption of Internet Banking. In *International Conference on Information Systems*. Brisbane, Queensland, Australia, 2000. Association for Information Systems Atlanta, GA, USA.

Kim, K. & Prabhakar, B., 2004. Initial Trust and the Adoption of B2C e-Commerce: The Case of Internet Banking. *Newsletter of the ACM SIGMIS Database*, 35(4), pp.50-64.

Legislation.gov.uk, 2000. Postal Services Act, Part V, Offences in relation to Postal Services. http://www.legislation.gov.uk/ukpga/2000/26/part/V, 2000.

London Economics, 2010. *Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs)*. Final Report to the European Commission DG Justice, Freedom and Security. London: European Commission.

Mishra, A.K., 1996. Organizational Responses to Crisis: The Centrality of Trust. In T.R. Tyler & R.M. Kramer, eds. *Trust In Organizations*. Newbury Park: Sage.

Moloney, M., 2013. The Postal Service: The Original Open System. *Working Paper Escher Group (IRL) Plc*.

Parker, G. & Alstyne, M.V., 2012. *A Digital Postal Platform: Definitions and a Roadmap*. Boston: The MIT Sloan School of Management.

Peters, R.G., Covello, V.T. & McCallum, D.B., 1997. The Determinants of Trust and Credibility in Environmental Risk Communication: An Empirical Study. *Risk Analysis*, 17(1), pp.43-54.

Rosenbaum, S., 2013. *Independence Day, NSA leaks inspire 'Fourth Amendment' rallies*. [Online] Available at: http://usnews.nbcnews.com/_news/2013/07/04/19287215-independence-day-nsa-leaks-inspire-fourth-amendment-rallies [Accessed 8 July 2013].

Rule, J.B., 2007. *Privacy in Peril*. Oxford: Oxford University Press.

Shankar, V., Urban, G.L. & Sultan, F., 2002. Online Trust: A Stakeholder Perspective, concepts, implications and Future Directions. *Journal of Strategic Information Systems*, 11, pp.325-44.

Teinowitz, I., 2011. *Trust of government agencies drops, but folks still love the USPS*. Media Report. WalletPop.com.

The Berkman Centre for Internet and Society, 2012. *Roadmap for Open ICT Ecosystem*. [Online] Harvard Law School Available at: http://cyber.law.harvard.edu/epolicy/home [Accessed 10 February 2013].

The European Commission, 1995. *EU Directive 95/46/EC - The Data Protection Directive*. [Online] Available at: http://www.dataprotection.ie/viewdoc.asp?DocID=89 [Accessed 11 November 2012].

The European Commission, 2002. Directive 2002/58/EC of the European Parliment and of the Council. *Official Journal of the European Communities*, 201, pp.37- 47.

The European Commission, 2009. Directive 2009/136/EC of the European Parliament and of the Council. *Official Journal of the European Union*, 337, pp.11-36.

The Ponemon Institute, 2010. 2010 Privacy Trust Study of the United States Government. *The Ponemon Institute Research Report*.

Triangle Management Services Limited, 2011. *Post Offices and Local Government Services – An International Literature Review*. [Online] Consumer Focus Scotland: Consumer Focus Scotland Available at: http://www.consumerfocus.org.uk/scotland/files/2011/08/POs-Government-Services-International-Comparisons-Final-Triangle-Report.pdf [Accessed 18th February 2013].

UN News Centre, 2013. *Online features essential for future of postal services – UN report*. [Online] The United Nations Available at: http://www.un.org/apps/news/story.asp?NewsID=41005&Cr=new+technologies# [Accessed 18th February 2013].

Universal Postal Union, 2011. *The Universal Postal Union*. [Online] Available at: http://www.upu.int/en/the-upu/the-upu.html [Accessed 29th April 2013].

US Postal Service Office of the Inspector General, 2013. *e-Government and the Postal Service*. [Online] (Report Number: RARC-WP-13-003) Available at: http://www.uspsoig.gov/foia_files/RARC-WP-13-003.pdf [Accessed 18th February 2013].

USPS.com, 2012. Who Protects you Mail? In *US Postal Inspection Service*. http://about.usps.com/publications/pub166.pdf, 2012.

Verizon.com, 2013. *The 2013 Data Breach Investigations Report*. [Online] Available at: http://www.verizonenterprise.com/DBIR/2013/ [Accessed 29th April 2013].

[1] In authentication, out-of-band refers to utilizing two separate channels, one of which is different from the primary channel, used to communicate between two parties or devices for identifying a user. An example of out-of-band authentication is when an online banking user is accessing their online bank account and to identify themselves they use a login and a one time password sent to their mobile phone via SMS.

[2] A database containing a collection of over 29 million Royal Mail postal addresses and 1.8 million postcodes in the UK (RoyalMail.com, 2013).