The Sealed Letter: Safeguarding the Public System of Privacy Protection in a Digital World

Liam Church
Escher Group
Liam.Church@EscherGroup.com

Maria Moloney
Trinity College, Dublin
Mmolone2@scss.tcd.ie

Frank Bannister
Trinity College, Dublin
Frank.Bannister@tcd.ie

Abstract

Amongst the casualties of the electronic age has been a number of institutions and the values and services associated with them. One example of such is the postal service and the concept of sealed, private correspondence. The universal postal service was one of the great social developments of the 19th century. Today, while such services continue to exist in almost every country in the world, much of the traffic that they formerly managed has been displaced by various forms of electronic communication. While this has brought benefits, it has also involved some losses. One loss has been the privacy of the sealed letter. This paper describes a project to develop a system to reinstate the concept of private correspondence in an electronic age.

1. The Nature of Public Service

The e-government literature contains a great deal on the subject of public services, but relatively little on the subject of public service. Possibly this is because the idea of public service is not seen as an ICT related matter or, if it is, then it is something best discussed by proxy through the lens of public services values [4],[23],[41]. Yet the idea of public service, of the community bearing the collective cost of delivering a service for the greater social good, is one of the fundamentals of a civil society [22]. Societies build their ideas of public service over long timescales. There was a time when, for example, free universal primary education would have been considered a strange idea. Another possible reason for the lack of discussion of public service in the e-government literature is that it can be a highly politicized concept: one person’s valued public service is another person’s excess government.

Like much else in life, the concept of public service is affected, and sometimes radically so, by ICT. One of the reasons for this is that any public service is based on some set of public values and these values often conflict [4]. This is particularly so when the service is both universal and either free or at a standard charge to all. Because technology can change the way in which a service is delivered, it can shift the balance between the values embedded in a public service and upset long accepted political and social trade-offs. When this happens, there can be collateral damage to other values as well.

One service so affected is the postal system. This paper considers this particular shift, the collateral damage that has resulted from this shift and a project designed, inter alia, to remedy that damage. In so doing, Rowley’s [31, p341] definition of e-services has been adapted to provide a definition of public e-services as:

“...deeds, efforts or performances whose delivery is mediated by information technology, including the Web, information kiosks and mobile devices, and are performed for the benefit of the public, society or its institutions. Such public e-services include both customer support and service, and service delivery”.

This definition provides both the concept underlying the project and the underpinning idea for the system described in this paper. It will also serve as a frame for a broader discussion and reflection.

The structure of the remainder of this paper is as follows. First some key ideas from the privacy literature will be reviewed. Next the nature of the postal service and its characteristics are discussed. The subsequent section briefly describes the research approach, which uses a combination of action research and design science, used to develop a new software product to address the concerns outlined above. The product, RiposteTrEx is then described. The paper concludes with some reflections on limitations, the future and on the wider implications of this project.

2. The Privacy Concept

Privacy has been declared as a fundamental right for every human in many enduring bodies of law [8]. Many IS researchers also deem privacy to be a human right [7],[37],[39].

However, a number of social scientists, such as Smith et al [35] and Solove [36], argue that the concept of privacy is in disarray as nobody can truly articulate
what it means. Numerous attempts have been made by social and legal scholars to bring together the different perspectives found in different fields. Nevertheless, the picture that emerges remains fragmented [35].

Table 1, adapted from Smith et al [35], summarizes the approaches to defining privacy that can be found in various disciplines. These approaches are classified into either value-based or cognate-based definitions. The value-based definitions view privacy as a human right integral to society’s value system. Historically, this was the first approach to defining privacy. Psychologists and cognitive scientists then became interested in a cognate-based conceptualization of privacy which was related to the individual’s mind, perceptions and cognition. When privacy is viewed as a state, it is logical for researchers to consider it in terms of its role as a sought-after goal.

The concept of privacy as a state was introduced by Westin [42] who defined privacy as having four distinct sub-states: anonymity, solitude, reserve, and intimacy. Later, Schoeman [32] defined privacy as a state of limited access to a person. Laufer and Wolfe [25] conceptualized privacy as a concept (state) tied to concrete situations with three dimensions: self-ego, environmental, and interpersonal. When privacy is viewed as a state, it is logical for researchers to consider it in terms of its role as a sought-after goal. The implication is that there must be a continuum of states of privacy, from absolute to minimal [35].

The control-based definition has since entered the mainstream of privacy research. This is possibly because it lends itself to the attributes of information privacy and has been further developed in the fields of information systems and marketing [35]. However there is a growing recognition that an individual’s understanding of what constitutes the modern concept of privacy includes having control over personal data [43].

| Table 1: Numbers of articles defining privacy as analysed by Smith et al [35] |
|-----------------------------|---------------|-------------------|------------------|-------------------|-------------------|-------------------|
|                             | MIS           | Philosophy, Social, Political Sciences | Law              | Psychology & Marketing | Economics         |
| Cognate based: Control      | 23            | 16                | 0                | 12                | 1                 |
| Cognate based: State        | 4             | 6                 | 0                | 0                 | 0                 |
| Value based: Commodity      | 17            | 10                | 1                | 2                 | 4                 |
| Value based: Right          | 12            | 24                | 25               | 4                 | 0                 |

The concept of privacy as involving the notion of control originated in Westin’s [42] and Altman’s [2] theories of privacy. Altman’s definition of privacy is “the selective control of access to the self” (p24). Margulis [27] unified and elaborated on Westin’s and Altman’s perspectives and proposed a control-centered definition: “Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability” (p10).

The control-based definition has since entered the mainstream of privacy research. This is possibly because it lends itself to the attributes of information privacy and has been further developed in the fields of information systems and marketing [35]. However there is a growing recognition that an individual’s understanding of what constitutes the modern concept of privacy includes having control over their personal data [43]. The notions of consent and the revocation of given consent form the basis for a new understanding of user-centric control of personal data [16]. This perspective of user-centric control is also prevalent in the literature of the European Union’s Internet strategy for the next decade [13]. Whitley [44] argues that this user-centric control of personal information is driven by the growing recognition, among policy makers and businesses alike, that providing users with control over their personal information is an important aspect of maintaining trust in an online environment. He argues, however, that the understanding of what user-centric control constitutes is not fully understood as it is based on earlier understandings of technology. Consent and revocation of consent regarding access to personal data facilitates a new form of control over personal data that has not been widely examined in the literature or in the practice of data protection.

Similar to Whitley, Van Dyke et al [40] have introduced the notion of ‘privacy empowerment’ to measure the effects of giving consumers more control over their personal data. They do not measure the actual construct of privacy empowerment; they use instead the proxy measure of ‘perceived’ privacy empowerment. Their results show that "those firms which meet the demand for control through empowering the consumer are rewarded with lower levels of privacy concern and increased trust" (p78).

In fact the premise that sustained rewards and business success cannot exist without respect for privacy protection in technology enabled innovation is growing in popularity even in the private sector [43]. Whitley [44] argues that corporate attitudes to personal privacy are changing. This argument is supported by revelations that Facebook employed a public relations firm to help plant negative news stories about Google’s privacy policies in the media [26]. Facebook’s actions.
suggest that how an organisation handles personal data is becoming a strategic rather than an operational issue. In fact, companies offering proof of online privacy protection such as displaying privacy seals on their websites, have been found to be able to charge premium prices for their products as a result [11], [44].

Despite pronouncements of its death [21], privacy remains an integral part of the social fabric and the protection and retention of appropriate privacy for those that need or want it is a major challenge of the digital age. One aspect of this is the privacy of personal communications.

3. The Nature and Role of Postal Services

Together with its numerous benefits, the digital age has brought its share of anxieties. One such group of concerns relates to the loss of socially valuable skills or behaviours (such as conversation [38] or social capital [30]). Other concerns surround the undermining, and in some cases loss, of valued services and institutions.

One example of the latter, i.e. of a service valued by people, but today increasingly threatened by technology, is the postal service. The first universal postal service was instituted in England in 1840 and from that time until the early 1980s, the typed or handwritten stamped and mailed letter was, alongside the telephone, the primary form of communication over distance. In most countries, the service offered by the postal system had a number of key characteristics. First it was regular, at least daily for most citizens and often more frequent in urban areas. Second it was both inclusive and universal. Anybody could send and receive letters. Third it was delivered to the customer at his or her home or workplace. This was true even in remote areas – at least in developed countries. Fourth, within the state, it was delivered at a standard price related only to weight and occasionally speed or registration. Fifth it was private. Letters could be intercepted and opened of course, but the privacy of the letter became an important feature of the service at least in democratic countries. Sixth, communication through the postal system was controlled according to the needs of the nation. This is particularly important from a privacy perspective as privacy varies from culture to culture (although social networking systems like Facebook may be erasing this characteristic). While postal systems are similar in many ways, each national system has adapted to suit the needs of its own citizens. Last, and by no means least, the postman and the post office provided a social infrastructure. In remote areas the post office, like the local library, provided a centre for communication, meeting and exchange. The low costs of using this system depended on, inter alia, economies of scale and low wage costs (it was and is a labor intensive industry). Universality depended on social cohesion, a form of what today might be called community rating, whereby those in expensive to reach locations were not penalized for their inaccessibility. The postal service could thus be considered as a social eco-system and, like all such ecosystems, it was vulnerable to disruption from technology. Table 2 summarizes these seven characteristics of traditional universal postal systems.

Table 2 Characteristics of a postal system

<table>
<thead>
<tr>
<th>Universal Postal Service characteristics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular and reliable</td>
<td>Daily delivery, the location of post offices in every town</td>
</tr>
<tr>
<td>Inclusive and universal</td>
<td>Anybody can send and receive mail</td>
</tr>
<tr>
<td>Delivered to a specified, private location</td>
<td>The customer can have mail delivered to their work or home, even if remote.</td>
</tr>
<tr>
<td>Delivered within the state, at agreed cost according to the wishes of the citizens</td>
<td>Delivered at a standard price related only to weight, speed or registration.</td>
</tr>
<tr>
<td>It is a private form of communication</td>
<td>The privacy of the letter was an key feature of the postal service in democratic countries</td>
</tr>
<tr>
<td>Controlled at a national level</td>
<td>Controlled according to the needs of each individual nation</td>
</tr>
<tr>
<td>Social infrastructure</td>
<td>Post offices and staff provided a center for communication, meeting and exchange.</td>
</tr>
</tbody>
</table>

Postal systems which possess these seven characteristics have provided the citizens of most nations in the world with a reliable and private means of communication for over a century and a half. By combining these seven characteristics citizens can exercise a degree of choice about the privacy of their personal communications. Three things underpin this.

Firstly, the legal protection of an individual’s own home prevents third parties from knowing when individuals open and read their mail. It is not (easily) possible to observe an individual’s actions in their own home though interested parties may be able to discover whether or not an individual’s mail has been delivered.

Secondly, in traditional systems of communication, citizens can choose to remain anonymous when going about their daily lives, until they choose otherwise. An individual’s method of written communication is disconnected from other areas of their lives such as shopping for food, meeting with friends or going to
work. Knowing an individual’s postal address does not link them to their other daily activities.

Thirdly, by being able to send and receive anonymous communication through the availability of post boxes and post office boxes, individuals can enjoy anonymous transfer of content. Suppliers do not need to know any personal information about the individual to supply products to them. The individual can anonymously request a product from a supplier and receive the goods via a numbered address. Thus, at least in the area of written communication, individuals could be as private or as public as they wished. The control of this aspect of their private life remains fully with them. Table 3 summarizes these three points.

**Table 3 Levels of Privacy Protection**

<table>
<thead>
<tr>
<th>Postal System Enabled Privacy</th>
<th>Privacy of the home</th>
<th>The postal system is disconnected from other areas of life</th>
<th>Anonymous receiving and sending of mail through a network of post boxes and post offices boxes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No one knows when an individual has read their mail</td>
<td>There is no link between an individual’s private communication and their other daily activities</td>
<td>Full anonymity through use of post boxes and post office boxes for transfer of content.</td>
</tr>
</tbody>
</table>

This is in distinct contrast to contemporary and evolving digital communication. With most public digital communications systems everything is public by default. The nature of the technology facilitates tracking of individuals and makes it straightforward for organizations to access, profile and target individuals for sales, marketing or other less ethical purposes. Organizations, particularly communication and information service providers (a term which includes companies such as Google and Facebook) have access to an ever greater amount of personal information about every individual with whom they come into contact online. The ability of the legal system to keep pace with this is limited. Laws have been put in place to prevent the abuse of personal information by organizations, but enforcing these laws is often impossible due to the transnational nature of modern on-line service delivery [12]. In addition to this, the current system shifts control of an individual’s ability to regulate their privacy needs away from the individual and into the hands of service providers and suppliers, disempowering the traditional ability of citizens to control their own privacy.

The explosion of the Internet and the Web into the public arena in the 1990s provided a number of new, fast and effective ways of communicating which this time posed a serious threat to the traditional postal service. e-Mail was soon followed by mobile telephony, SMS texting, social networking, Twitter and Voice (Video) over Internet Protocol (VOIP). These new means of communication offered a number of advantages, especially in speed and price, which the traditional postal service could not hope to match. But these gains were achieved at a cost. Of the seven characteristics of postal services set out above, the following in particular were threatened: privacy, both in personal data storage and data transfer, was threatened as were inclusiveness, national control of communications and the social infrastructure provided by the postman and the network of post offices. This paper is concerned primarily with the first of these, the threat to (or actual loss of) privacy, but it will also be argued that in order for society to achieve a fully private communication system, in line with the universal postal system, at least two of the other threats (national control of communications and inclusiveness) also need to be considered and attempts made to reduce threats to their continued existence. In what follows, we present this argument in more detail and describe a project and a product which seeks to address these problems and deliver an on-line product which can provide something approaching the traditional mailed letter experience.

**4. Research Methodology**

This is a continuing project and the methodology which uses Action Design Research (ADR) integrated with the concept of engaged scholarship [9]. Space limitations preclude a discussion of the latter, but the key aspects and role of ADR as used in the project are outlined in this section.

ADR can be used in a number of ways. For example, the ADR method has been shown to facilitate the reconfiguring of organizational IS functions, making them more efficient and effective in supporting organizational needs [33]. When used in New Software Product Development (NSPD) however ADR supports agile development. The last decade (2002-2012) has witnessed a continuing debate between proponents of traditional and modern approaches to software development. This conflict is most evident in the debates over Software Process Improvement (SPI) and Agile Software Development (ASD) [1]. At the centre of these debates are distinctions between predictable manufacturing and new product development, which according to Aaen [1] reflect recent developments in software technologies that appear to be having an effect on software innovativeness. Aaen asserts that traditional software development aims for predictable and documented production, while agile development aims for innovative and dynamic development.
Like traditional methods, agile software development also uses iterative development, but it promotes a lighter and more user-centric approach. Agile processes employ user feedback rather than planning as their primary control mechanism. Agile development focuses on customer involvement via the whole team [5], emergent design [14] and test-infected development [6]. It sees testing as confirming that user and customer needs are met [1]. Agile development is faster paced and focuses on adaptive planning with built-in feedback loops, and is based on incremental development with more frequent releases [24]. Figure 1 shows how the start and initiation of an agile software development lifecycle is immediately followed by the construction of the software.

When ADR is used in a NSPD environment, the challenges differ slightly. In such an environment, ADR does two things. First it addresses a need or service requirement encountered in a specific real-world setting that has not yet been met by information technology. Second it constructs, modifies and evaluates a software product that addresses the need or requirement and continues to do this until and after the software product goes to market. The feedback from the first release can be used to test feature design and help improve marketing and customer support [20].

![Figure 1 Agile software development lifecycle (adapted from [3])]}

Sein et al. [33] set out four stages in, and seven principles which underline, ADR. While the ADR approach used in the RiposteTrEx development project follows the four stage structure outlined by Sein et al, an additional fifth stage was added to the final part of the ADR project reflecting the view that the ADR method should continue until the software system has been fully validated by the users. Sein’s model has also been extended by the addition of an eighth principle. This structure is illustrated in figure 2. A detailed discussion of this is beyond the scope of this paper, but the application of the stages and the principles in the RipostTrEx project is discussed in the next section.

![Figure 2 Extended ADR methodology]

### 5. The RipostTrEx System

The RipostTrEx system is designed to deliver a number of aspects of public service value. While the focus in this paper is on privacy, it is useful, briefly, to sketch the wider context. The system is built using a number of design principles collectively called the Public e-Service ICT (PeSICT) design theory [28]. A summary of this theory is shown in table 4.

The framework incorporates a set of four design principles, divided into two categories: public social system principles and public software system principles. The aim of the design theory is to provide a method for the production of ICT applications that provide inclusive public e-services. The principles of relevance to this paper are groups one and two, the principles for Equal Control and Equal Access to a privacy-enhanced public communications system.

![Table 4 Outline of Design Principles for the PeSICT design theory.](data:image/png;base64,)){"width":300,"height":200}}
5.1 Principles for Equal Control

This section looks at the first set of principles relating to equal access to personal information by both interested parties and the individual to which the personal information pertains.

5.1.1 Secure and Private Data Storage Units. One of the original motivations behind the design and development of RiposteTrEx was to give control of his or her personal information back to the individual and thus help reduce online privacy concerns. In order to satisfy this central principle four sub-principles need to be addressed. The first of these is secure and private data storage units (SPDSUs).

When providing a public communications system, it is essential to ensure that all private information that passes through the system is securely transferred and stored. This is particularly relevant for public e-services provision as the data processed and stored within the system can be extremely sensitive (e.g. financial and health information). Were the security of such information to be compromised, there would be real potential for harm. There are three levels of security that need to be implemented to ensure comprehensive, effective security: access security, communications security and data security.

Access security entails ensuring that access to the data storage units are secure. With RiposteTrEx, there is only one service that can access the SPDSUs and this is done at the application level of the system. All users access the system via the RiposteTrEx Interface which then accesses the SPDSUs via a secure socket layer (SSL). SPDSUs can be stored within the RiposteTrEx infrastructure or can be stored at other locations provided by other service providers (SPs). No matter where they are stored, access to the SPDSUs is still only possible via the RiposteTrEx Interface. Figure 3 shows this secure configuration.

Communications security is achieved by ensuring all communications between RiposteTrEx on the one hand and users or other SPs on the other are run through SSL.

Data security is achieved by ensuring compliance with industry standards such as the Payment Card Industry Data Security Standard [29]. This standard provides a framework for developing a robust payment card data security process. This includes prevention, detection and appropriate reaction/response to security incidents. For further details on this process see [29]. The principles of data minimization and minimal retention are applied to any personal data stored within the system. For an account of these principles, see [15].

![Figure 3. Security Architecture for RiposteTrEx](image)

Once a SPDSU has been set up for a citizen within the system, there is no need for additional SPDSUs to be set up for that user by any other public sector body that joins the network at a later stage. Unless otherwise specified by the individual the same SPDSU can serve as a storage unit for all information pertaining to that user transferred and/or stored within the system.

Each user of the RiposteTrEx system is allocated SPDSU for storing their personal information. There is also an option to compartmentalize the data within SPDSU according to the stated privacy preferences of the individual.

5.1.2 Independence and Separation. An important design feature of the system is that it must be transactional and message-based in nature in order to ensure each user’s interactions are separate and independent of each other. In this way every user of the system has an historical record of their actions and transactions. This is unlike the asymmetrical situation when users visit a typical commercial website. Website
owners can (and often do) track the movements and transactions of the user, but the user has no comparable comprehensive record of their own movements or transactions. By ensuring the system is message-based and transactional, identical records of all actions taken are available to both parties.

5.1.3 Choice and consent for citizens regarding their personal information. While data ownership can be a complicated question, in principle at least, control of a citizens’ personal information should be in the hands of the owner of that information, i.e. the citizen to whom the information relates [10]. All citizens of a nation should be able to access, process, store and transfer their personal information irrespectively of which SP they are using. To achieve this, citizens need to be able to do two things. First they need to be able to choose their preferred location for storing their SPDSU. Other SPs should be allowed to compete for storing these units in their systems provided they meet all the requirements for ensuring the appropriate transfer and storage of personal information. The latter would include receiving consent from the citizen to use their personal information for any reason. Second, the SPs need to be able to enable citizens to retain copies of all the transactions they carry out through the system. In this way citizens can if they wish extract information regarding their online activities such as monthly financial expenditure.

Such public e-service systems must allow other SPs to inter-operate with the system. As the system grows, legally regulated service level agreements (SLAs) can be devised between governments and third party SPs so that private sector SPs offering appropriate storage facilities and extra value-added services can partner with governments to extend the range of service offerings to citizens. It is important to note that SLAs between the public sector and private SPs will need to be clear on the question of ownership of personal information generated within an SP’s systems. Ownership must remain with the citizen to which the information relates. Licences which provide permission to use such information can then be issued to the SPs for an agreed price.

5.1.4 Online trust and privacy assurance. Akin to the privacy of correspondence in the paper world, users of a public communications system may require that the content of messages are not altered and are disclosed solely to the recipient.

A challenge for the RiposteTrEx project was to assure the users that they could trust the technology that electronic posts on the system can provide. To achieve this RiposteTrEx supports an optional end-to-end encryption, which ensures confidentiality between the sender and the recipient. Protection should be assured for both personal data and for unique national identifiers to ensure adequate levels of anonymity for both the user and his or her location. In de jure systems the handling of sensitive data is regulated by national laws. These include procedures surrounding the disclosure of personal data through lookup services within the system as well as the disclosure of personal data to third parties [45]. It is of critical importance that public communication systems do not allow inappropriate disclosure of sensitive data through technical, legal and organizational provisions [45]. This encourages and maintains trust between the service provider and the citizen.

5.2 Principles for Equal Access to a Privacy-Enhanced National Communications System

The second set of principles is the provision of equal access to a public, privacy-enhanced national communications system for all citizens.

5.2.1 Education of citizens on how to safeguard their privacy. Citizens who have had no training in electronic devices and are afraid of going online due to fear of viruses, breach of personal information resulting in loss or theft of their personal belongings or just fear of the unknown can avail of public access points in post offices. Training courses on how to use the digital communications system can be provided by post office staff. It is planned that once RiposteTrEx is commercially available these access points will be rolled out in a phased schedule. For more proficient users of technology, RiposteTrEx is available in the form of a mobile phone app.

5.2.2 Interoperability and transparency Service architectures, protocols and interfaces need to be standardized to ensure interoperability, transferability and reusability with other systems. This facilitates the deployment of an integrated public communications system and allows both the private and public sector to collaborate on development efforts so as to provide more and improved services to citizens via the public communication system. This should lead to an increased level of system up-take by citizens. Open standards also ensure transparency and freedom of choice. This can be beneficial when considering cross-border interoperability. The ETSI Registered E-mail Standard defines a common format for developing certified electronic mailing systems to ensure system interoperability with standardized extended markup language (XML), Content Management System or PDF
files. RiposteTrEx uses the Simple Object Access Protocol (SOAP) web service specification with backwards compatibility to ensure connectivity for legacy systems [17],[18],[19].

5.2.3 Neutrality: Managed in an impartial and unbiased manner. It is essential that the provider of the public communications system does not exploit the personal data of their customers. Research has shown that given the profit-driven and competitive nature of our digital society and individuals’ concerns surrounding issues like the protection of their personal information, individuals prefer to entrust their personal information to familiar and trusted brands. However, research shows that not all citizens will be happy to allow a government body to store their personal information. Therefore, a requirement of a public digital communication system must be to ensure that citizens can decide where their personal information is stored i.e. either within the system of a private service provider (SP) like a bank or telecommunications company, with a public/private company like the postal service or with a government department or agency.

5.2.4 A national de jure system. A national de jure system means that the system has been developed in the context of e-government and therefore operates under particular national laws. De jure systems provide services for Non-Repudiation of Submission (NRS) and Non-Repudiation of Delivery (NRD). The former provides public authorities with evidence of the delivery of a mail item having taken place at a certain point in time. The latter provides public authorities with evidence that mail was delivered to a recipient at a certain point in time. This is similar to the conventional postal service in that if required, receipt of delivery can be specified. But this is only delivery, it does not notify the sender when the mail is opened. This does not affect the individual’s right to decide to open the mail or not. Individuals can still send and receive mail anonymously through the system by choosing to withhold sender information when sending messages. The intended recipient would know the sender when (s)he opens the mail, but a third party would not be able to establish who sent it. By default the contents of mail are encrypted.

Implementation guidelines concerning non-repudiation protocols are specified by the ISO/IEC standards [18],[19],[20]. RiposteTrEx is built upon an existing postal architecture which has been used for over a decade by post offices globally to electronically interact with each other.

6. Limitations and Future Development

Action design research presents a particular set of methodological challenges and limitations. Three challenges which proved significant during the RiposteTrEx project were funding, personnel and technical problems all of which diverted management and staff effort. One unanticipated problem was that the traditional development environment used by the developers of the company for other software products proved to be insufficiently flexible for developing the RiposteTrEx architecture and as a result a completely new development environment had to be designed and created to complete the task.

A key question for a service of this nature is how it will be financed? There is a price for posting a letter; e-mail is as close to being free of charge as to make no difference. And while a service like RiposteTrEx will cost only a tiny fraction of the cost of putting a stamp on a letter, it obviously will involve an additional layer of cost above that of current, but insecure, e-mail systems. On the other hand, in comparison with current encrypted e-mail RiposteTrEx is highly competitive. Virtual private networks and public key interface systems are expensive to set up and maintain and while point to point encryption can be relatively inexpensive, the key management involved is impractical for individual users.

The critical question is, therefore, how much will this cost the user and whether the user is prepared to pay for this service? e-Mail might appear ‘free’, but users need first to invest in equipment, broadband access and software. A once off or small annual charge for secure e-mail option might not be significant in this context. The Irish postal service, An Post, which is sponsoring this project clearly feels that there is a potential market for such a product. RiposteTrEx’s success will ultimately depend on the ability to deliver a product that is easy to understand, modestly priced and seamless to use as well as on a growing public awareness of the risks to their privacy of current e-mail systems. The RiposteTrEx system has recently been piloted by two government agencies in Ireland. One of the pilots is still ongoing; the other has led to the system being deployed for large scale use within the piloting agency. A number of research projects are ongoing which are looking to adapt the system for various other domains that require high levels of security, such as e-health and assisted living networks.

7. Conclusion

When considering how the type of communication provided by the RiposteTrEx system compares to traditional systems a number of observations can be made. First, in the traditional system the legal protection of an individual’s own home prevents third
parties from gathering excessive information about the individual. In RiposteTrEx the secure and private data storage units provide a similar form of protection in the digital world. Secondly just as in traditional mail systems the RiposteTrEx network is closed from the larger World Wide Web thus providing a similar form of insulation. Users browsing the Web through the RiposteTrEx network are much more difficult for third parties to track and profile as critical information such as IP addresses are withheld. As a result, individual must actively provide the personal information they choose to provide in contrast to this information being gathered without their knowledge and consent. Thirdly, while RiposteTrEx cannot provide complete anonymity for individuals in the digital world (due to the fact that currently in order to pay for items electronically credit card details must be provided) it does, provide individuals with a means of digital communication that allows them both to send privately and to store securely sensitive information such as health records and disconnect the storage of such data and activities related to them from their other daily online activities. By creating such a disconnect individuals can start to enjoy increased online privacy.

Not everybody is sensitive about the privacy of their data. Individuals range from what Sheehan calls the privacy unconcerned to the privacy alarmed [34]. But for the sizable section of the population for which on-line privacy matters, RiposteTrEx and the concepts and technology which underlie it offer one way of achieving their privacy goals. Considering our digital identity consists of nothing else but an amalgamation of (sensitive) personal information, finding a means to disconnect items of personal information from each other and thus increase online privacy should be of paramount importance.

6. References


