Informational Privacy Preservation through Universal Service Obligations

Maria Moloney
Trinity College Dublin
Dublin 2

Liam Church
Escher Group Holdings Plc
Dublin 8

Abstract

The argument in this research is that the Universal Services Obligation (USO) has endured for, and evolved over centuries, instead of reducing the USO in our digital world, it should be strengthened and redefined to ensure all members of society enjoy the full benefits of the new emerging digital world. This is particularly important at a time where research into new electronic services is in great demand and the submission of private information via electronic means is causing mounting privacy concerns among the public.

1. Introduction

Since the 1970s, governments across Europe, and indeed elsewhere, have held the belief that public bodies were best managed like private businesses. This has resulted in a number of key government policy shifts to replace state services with numerous competing providers [1]. This approach has impacted upon how public services are currently offered to the public. Moreover, with the onset of the digital revolution, public services are being redefined and transformed in an attempt to suit citizen's evolving needs, with little regard for the USO [2]. While redefining the USO is largely a regulatory issue, researchers and practitioners in the domain of public service provision should understand how their roles change as citizens move online. Similar to the concept of trust, the USO is likely to be different in digital form [3]. In this embryonic environment important social values, such as safeguarding the notion of privacy, can get overlooked. This paper argues that ICTs are not neutral instruments. Even when designers of ICTs try to deliberately design values into systems, what emerges often gets used in different ways from the designer's original intentions. This effect is described by Bannister and Connolly [4] as the law of unintended consequences. The result of these unintended consequences of technology can often lead to positive and beneficial outcomes, but sometimes the unintended consequences can have negative repercussions. In such scenarios, protections should be put in place to ensure that these negative consequences are identified and rectified as soon as possible.

2. Literature Review

De Reuck and Joseph posit that the concept of a USO is relative to the historical moment in which it occurs. That is to say that it is not a rigid concept but rather a dynamic one, which requires continual revisiting in light of changing technological innovations and social needs [2]. In fact in recent years, many countries have been redefining the term "Universal Service" according to their changing national telecommunications needs and the evolution of modern technology. New "Universal Service Support Funding Mechanisms" have even been developed in some countries [5]. In the United States, the Telecommunications Act of 1996 defined universal service as an evolving concept [5], and in Great Britain and Finland, the provision of broadband services to all households in the country has recently become a universal service [6,3]. It is argued here that the USO should be extended to encompass some vital e-services to ensure the rights of citizens are considered when doing business online.

Let us develop this argument further. Research has shown that given the profit-driven and competitive nature of our digital society and individuals' concerns surrounding the protection of their personal information online, individuals prefer to entrust their personal information to familiar and trusted brands [7]. When individuals 'trust' an online brand, it increases the likelihood of those individuals interacting with that brand because trust alleviates concerns regarding possible negative consequences [8]. Research also shows that in recent decades there has been a decrease in public trust for the government [9]. The challenge now facing public bodies is to regain citizens' trust in both the digital and physical worlds.

The USO is a recognised and trusted symbol of any democratic society. Thus, expanding this democratic symbol to encompass the new digital world has the potential to increase citizens' trust in their government. While most modern USOs ensure a minimum speed connection to the Internet for citizens, little mention is made of protecting citizens' democratic rights when availing of e-services, especially in regard to the protection of their private information that is often required in exchange for an e-service.

It can be argued that many services once provided by the government in the physical world are now being replaced by digital equivalents in the hands of private companies. Some examples of these are email replacing postal mail, Google maps (largely) replacing ordinance survey maps and the national public telephone directory is now available through Internet search engines such as Yahoo and Google. A significant consequence of this is that, unlike regulated governmental bodies, private enterprise is not held accountable to the same degree as public bodies; they are not subject to national administrative law or to the freedom of information act. Consequently, transparency and accountability in e-service provision can potentially be eroded. There is a key consequence of this for the citizen. Namely, citizens have growing privacy concerns regarding their personal information within the digital world [7]

Even though governments provide digital equivalents for some of the e-services offered by the private sector, i.e. directory services instead of search engines, given the profit motivation and advertising strength of these companies, the privately owned digital equivalents are developing faster and capturing a larger portion of the market. As a result, governments are no longer competitive. Yet, it should not be overlooked that by allowing a private monopoly to develop, citizens' basic democratic rights to vital, affordable, inclusive public services *could* be threatened. In reaction to this situation, various approaches to reforming public services have been proposed whereby public bodies can deliver efficient services, while still remaining publicly accountable [10].

Realistically though, many e-services which benefit the citizen have already become established by private companies. At present, all personal information that private Internet companies aggregate about citizens is administered for the sole benefit of the Internet company, not the individual. While these Internet companies may be obliged by law to disclose any personal information they hold on an individual, it is still difficult for an individual to see the extent of the personal information stored about them by these companies. The legal case taken by an Austrian law student at the University of Vienna against the social networking company, Facebook demonstrates this difficulty [11]. Ascertaining the breadth of the stored data is not a transparent process. Understanding how the Internet companies are using this data is even more difficult to ascertain.

Already the consequences of these challenges are evident. Citizens have growing privacy and trust concerns regarding their online personal information which is in the hands of these companies. Unfortunately, it has been argued that at this stage, providing equivalent services with technologies that protect the personal information of citizens is both a mamooth and futile task. Perhaps finding alternative solutions to these challenges now needs to be examined. This paper sought to elucidate some of these alternatives. To help with our endeavour, the help of the public was sought through the use of focus groups.

3. Analysis of Findings

Eight focus groups each consisting of eight people were set up. Participants of the focus groups were selected from a mailing list of a professional research company. Gender, age and socio-economic status was considered when making the selection. People with personal computers and without were included, unemployed people and stay at home mothers also formed part of the list of participants. Each focus group lasted 90 minutes. This paper reports the initial findings of the focus groups and work is continuing on analysing the thick data that has been gathered from these meetings The following two questions were put to the eight groups:

1. *Will providing more publicly run e-services help reduce the online privacy concerns of citizens?*
2. *How can we redefine/transform the USO to reduce online privacy concerns of citizens?*

To start with, 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. Finally, they were asked to give possible solutions to the questions above.

4. Discussion

Regarding the resolution of online privacy concerns, the initial finding of the focus groups was that while individuals accept that the digital world is not perfect regarding safety and the protection of personal information, it has brought more benefits than challenges. Even individuals who proclaimed to be either concerned about or aware of the challenge of safeguarding their online privacy, agreed on this. Participants of all ages, gender and socio-economic backgrounds also agreed with this point of view. It was found that as the age of the participants increased, the more important the issue of online privacy became. People who used the Internet frequently saw how finding solutions to online privacy concerns would be beneficial whereas people who infrequently used the Internet did not see any added 'personal' benefit to resolving such a challenge. In fact, some even went as far as to say online privacy was not a challenge but simply an ideal. Individuals who owned or worked in businesses that frequently used the Internet saw a huge benefit to resolving this issue and generally believed their business would benefit from the issue of online privacy being resolved.

Another general finding of the groups was that private companies were perceived as an equal or greater threat to individuals' online privacy as government or public-private partnerships. Even though participants were sceptical by nature of their personal information being correctly used online, they were more willing 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 [12]. 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 recent 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) [13].

Another significant finding was that, participants did, however, have reservations about the technical competencies of public bodies to safeguard private data. 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 [14] 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. [15] who, when analysing 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. [16] demonstrate a positive correlation between satisfaction with public services and trust in public services.

Interestingly, it was also found that when the users interacted with public-private partnerships, they felt more in control of their data than when they interacted with either government or private enterprise individually. This would suggest that using a public-private partnership to protect private information online would help to reduce online users' privacy concerns. This finding is supported by the Ponemon Institute [17] in the United States which 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) first among the 75 agencies. This is the sixth year running that USPS has won this award. Ranking first indicates that Americans trust USPS to keep their information safe and secure [18]. According to the laws under which the USPS now operates, the U.S. Postal Service is a semi-independent federal agency, mandated to be revenue-neutral [19].

The suggestion that governments should oblige private companies under the USO to safeguard, defend and respect the personal information of citizens from whom they have collected information was welcomed by the majority. The challenge of enforcing this new USO was also widely acknowlegded

5. Conclusions

Arguably, over the last two or three decades, government policies of prioritising market competition over democratic goals have subtly but progressively affected citizens of numerous countries. As a result of a decline in demand for traditional unviersal services such as the postal service, governments in Europe and worldwide have reduced their universal services obligations instead of adapting them for the digital age. If there is to be a truly safe digital society, a series of amendments to the traditional USO is required along with the amendment of legislation both at a national and international level to support these new universal services.

By bringing universal services into the digital world, citizens can experience the benefits of publicly inclusive services in digital form. Governments would also reap benefits in the form of increased societal trust and an affirmation of their democratic role in modern society. The entire community would benefit through full and safe engagement with both their government and digital society.

This paper presents some possible solutions to the challenge of data protection online. From the literature review and analysis of data gathered from eight focus groups, the authors present some novel suggestions to alleviate the challenge of online privacy protection such as the suggestion that using a public-private partnership to store and protect private information online would help to reduce users' online privacy concerns.

6. References

[1] Hood, C.: A Public Management for All Seasons? Public Administration 69(Spring), 3-19 (1991)

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

[3] Parker, G., Alstyne, M.: A Digital Postal Platform: Definitions and a Roadmap., The MIT Sloan School of Management, Boston (2012)

[4] Bannister, F., Connolly, R.: Transformation and Public Sector Values. In : t-Gov Workshop (tGOV11), London (2011)

[5] Zhang, B., Li, X., Taylor, R.: Universal Service Reform In The U.S. And China: Sustaining The Social Balance. In : Pacific Telecommunications Council, Honolulu, Hawaii, USA (2007)

[6] Carter, L.: A User's Guide to Digital Britain.

[7] Belanger, F., Carter, L.: Trust and risk in e-government adoption. Journal of Strategic Information Systems 17, 165–176

[8] Kim, K., Prabhakar, B.: INITIAL TRUST, PERCEIVED RISK, AND THE ADOPTION OF INTERNET BANKING. In : International Conference on Information Systems, Brisbane, Queensland, Australia , pp. 537 - 543 (2000)

[9] Morgeson, F., VanAmburg, D., Mithas, S.: Misplaced Trust? Exploring the Structure of the E-Government-Citizen Trust Relationship. Journal of Public Administration Research and Theory 21(2), 257–283 (2011)

[10] Cordella, A., Willcocks, L.: Outsourcing, bureaucracy and public value: Reappraising the notion of the 'contract state'. Government Information Quarterly Volume 27(Issue 1), pages 82-88 (January 2010)

[11] Lillington, K.: Facebook faces up to the data commissioner. In: Irishtimes.com. (Accessed January 6, 2012) Available at: http://www.irishtimes.com/newspaper/finance/2012/0106/1224309884789.html

[12] Dinev, T., Hart, P., Mullen, M.: Internet privacy concerns and beliefs about government surveillance – An empirical investigation. Journal of Strategic Information Systems 17, 214–233 (2008)

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

[14] Kim, K., Prabhakar, B.: Initial Trust and the Adoption of B2C e-Commerce: The Case of Internet Banking. Newsletter of the ACM SIGMIS Database 35(2), 50-64 (2004)

[15] Kelly, G., Mulgan, G., Muers, S.: Creating Public Value. An Analytical Framework for Public Service Reform. In: Cabinet Office UK. (Accessed 2002) Available at: Strategy Unit discussion paper accessed at: http://webarchive.nationalarchives.gov.uk/+/http://www.cabinetoffice.gov.uk/strategy/downloads/files/public_value2.pdf

[16] Grimsley, M., Meehan, A., Green, G.: Social capital, community trust, and e-government services. In : First International Conference on Trust Management, iTrust , Heraklion, Crete, Greece., pp.28 - 30 (2003)

[17] Accenture: How Global Organisations Approach the Challenge of Protecting Personal Data., In conjunction with the Ponemon Institute LLC (2009)

[18] Teinowitz, I.: Trust of government agencies drops, but folks still love the USPS. Media Report (2011)

[19] Longley, R.: About the U.S. Postal Service: A Very "Business-like" Semi-governmental Agency. (Accessed August 21, 2012) Available at: http://usgovinfo.about.com/od/consumerawareness/a/uspsabout.htm

