

Personalisation

MANAGING CONSUMER CHOICE AND PRIVACY

Key Findings

- How our digital footprints are collected and managed by the organisations we have relationships with will have long term implications.
- The promotion of privacy issues and the importance of the protection of personal information is critical to ongoing functioning of the online environment.
- Data gleaned from previous engagements is used to determine the differences between individuals - personalisation.
- If done right, personalisation will be the “Customer service” of the 21st Century.

The key questions every business (and privacy regulator) must ask themselves are:

Does the customer

- know what data is being collected?
- know what the data will be used for?
- know who will have access to it?
- give consent - informed consent - for it's collection?
- have the ability to opt out of such data collection and still be able to use the service?

Introduction

The promotion of privacy issues and the importance of the protection of personal information is critical to ongoing functioning of the online environment. As part of this dialogue we should consider how privacy is impacted by rapid changes in technology, in particular the phenomenon of “personalisation”.

Today, almost all individuals have digital footprints, created via interaction on social networks, through search, participation in eCommerce and other online activities. Technology can deliver significant benefits, but we need to take care: how our digital footprints are collected and managed by the organisations we have relationships with will have long term implications.

Global CEO of eBay, John Donahoe, indicated eBay was heading in that direction in comments made to an analysts meeting in March 2013: “There’s going to be an enormous jump around giving a consumer a more engaging, personalized experience...We are absolutely focused on innovating and experimenting -- it’s a natural place for eBay to thrive.”¹

eBay is not alone in this quest.

About the Authors

Alastair MacGibbon is an internationally-respected authority on cybercrime, including Internet fraud, consumer victimisation and a range of Internet security and safety issues. For almost 5 years Alastair headed Trust & Safety at eBay Australia and later eBay Asia Pacific. He was a Federal Agent with the Australian Federal Police for 15 years, his final assignment as the founding Director of the Australian High Tech Crime Centre.

Nigel Phair is an influential analyst on the intersection of technology, crime and society. He has published two acclaimed books on the international impact of cybercrime, is a regular media commentator and provides executive advice on cyber security issues. In a 21 year career with the Australian Federal Police he achieved the rank of Detective Superintendent and headed up investigations at the Australian High Tech Crime Centre for four years.

About the Centre for Internet Safety

The Centre for Internet Safety at the University of Canberra was created to foster a safer, more trusted Internet by providing thought leadership and policy advice on the social, legal, political and economic impacts of cybercrime and threats to cyber security.

The Centre for Internet Safety is hosted within the Faculty of Law at the University of Canberra. The University of Canberra is Australia’s capital university and focuses on preparing students for a successful and rewarding career.

www.canberra.edu.au/cis

¹ <http://www.bloomberg.com/news/2013-03-28/eBay-expects-110-billion-in-merchandise-volume-by-2015-1-.html>

Personalisation

When we visit a cafe we've been to many times, and the owner greets us by name and ushers us to our favourite booth while the barista starts to prepare the coffee we normally order, we see this as excellent service, in fact quintessential customer service. It's hard to imagine a scenario where we would feel uncomfortable about this sort of behaviour: it is flattering, fast, and often just what we want.

But we don't necessarily want the receptionist at a medical practice to ask about (nor potentially even know) our chronic ailments in front of other patients. In fact, service in that environment may be explicitly not talking about our medical condition, but instead treating us as a welcome and valued visitor while helping complete administrative paperwork and waiting to see a doctor.

It is relatively simple offline: the concept of personal customer service, and what's appreciated and not appreciated, will vary depending on the environment we are in, the nature and extent of our past dealings with the business, and - of course - our personal preferences. For their part, businesses need to be attentive to societal norms and social cues exhibited by their customers, as well as any professional or legal restrictions on certain behaviours.

One way services are attempting to innovate online is to personalise what customers see:

personalisation. Personalisation seeks to satisfy the needs of individuals. Data gleaned from previous engagements is used to determine the differences between individuals. Results are (theoretically) relevant to the individual user, based on the user's implicit behaviour and preferences, and explicitly given details.²

If there is one thing that's certain, it is that online interactions with customers can generate an amazing array of specific and general data which, depending on the service - if signed into an account, or linked by cookie, for example - can be tied to an individual. When an online interaction is carried out via a mobile device, such as a smartphone or tablet, as an increasing amount are, another incredibly rich set of data can be captured, including location (which would give companies insights into the temperature and weather where the user is, the shops and services they are near, who else is near them, etc).

Personalisation is already taking place through facial recognition technology. This technology enables automatic identification or verification of a person from a digital image or video source. One way of doing this is comparing other facial features within a database which some social networks use. These technologies have traditionally been used in the defence or law enforcement sphere, but has been extended for other purposes. With so many cameras and photo sharing applications, facial recognition will

² <http://en.wikipedia.org/wiki/Personalization>

have growing commercial and social importance.

The convergence of online technologies means individuals can be more easily tracked, monitored and profiled. Organisations wishing to collate this data and interpret it can provide very personalised consumer services and experience.

Traditionally, organisations who offered personalised services, could charge a premium for their goods or services. The personalisation of online activity has now become a necessity to acquire and retain customers, who are spoilt for choice. Personalisation in the online context relies on the knowledge of a consumer and the ability to cater to their needs. It can happen on any internet-connected device, mobile phone or television and extends to online shopping, advertising shown to the individual³, news⁴, as well as other content.

Societal Norms

There are many privacy concerns surrounding the collection and use of the information contained in the digital footprints we leave during online transactions. However to put this in context we need to understand the length and nature of the relationship between a customer and, for example, an e-commerce website. We also need to understand how such information is collected and the context of which it is likely to be used.

When our barista remembers our coffee order we appreciate being treated as an individual and such attention is traditionally seen as offering superior service and complements our experience. This social exchange is accepted by consumers and with it they are only divulging minimal personal information.

A notional scenario of how this may work on eBay is: a regular eBay buyer purchases a tablet device, following the purchase they may be offered a promotion regarding the opportunity to purchase an accessory item related to the tablet for example a tablet cover, or headphones. Just like the coffee shop or medical practice, this transaction has been personalised, however the vendor will only retain the trust and confidence of the buyer if their personally identifying information is not indiscriminately sent to third parties. So whilst there is no guarantee of future economic advantage for eBay, this personalisation is both discrete and social.

By way of difference, our relationship with the medical practice is more complex. Even though we may have had a similar length of commercial relationship, it is more discrete, (as opposed to social) and is more structured (as opposed to informal). However in both these scenarios there is an implication none of our information is shared with third parties.

Repeated exchanges (whether online or offline) over time

³ Also known as “online behavioural advertising”

⁴ See, for example, Facebook’s efforts to personalise it’s news feed <http://au.businessinsider.com/facebook-unveils-new-news-feed-2013-3>

generate trust in both commercial and social transactions. However the repeated online exchanges are characterised by greater collection of transactional and personal information, thus leading to the ability to deliver personalised service. Accordingly such collection induces privacy concerns which may negatively affect future exchanges.

A 2012 Accenture survey found 75% of online shoppers prefer retailers that use personal information to improve their shopping experience.⁵ The same survey found 61% would trade privacy for personally relevant offers.

Consumer knowledge and perception of privacy is an individual measure. The perception of privacy in an online transaction may be measured by a consumer's concern with the probability of their personally identifying information being collected, accessed and disclosed in accordance with societal norms and personal expectations. What is unknown is how much consumers are willing to give up this concern for an economic or social benefit.

Personalisation is a function of an organisation's knowledge of a customer. Collection of data will always warrant consideration of the privacy implications and concerns by consumers, businesses and regulators - and

brings significant obligations to the entity collecting the data.

Legal Restrictions

Like the offline world, online organisations are liable for the collection and retention of customer information. Given the increased amount of information collected and the number of actors involved, sensitivity and liability are key legal concerns. Online consumers should not be misled about what their data will be used for.

Both the Singaporean⁶ and Australian⁷ Governments, amongst others, have started discussing the issue of how "big data" can be used to better deliver services to their citizens, with an Australian Government discussion paper saying "This granularity may assist in unlocking the possibility of personalised services tailored to the individual and delivered by government." Big data relates to organisations collecting and mining voluminous quantities of data to not only exploit them for new purposes, but also piece together personal information.⁸

In 2010, the Hong Kong government launched a 'personalised and integrated' e-government service delivery platform – developed by the Office of the Government Chief Information Officer to provide more citizen-centric services to residents and visitors.⁹

⁵ <http://www.accenture.com/us-en/Pages/insight-shopper-preferences.aspx>

⁶ <http://www.ida.gov.sg/~/-/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/BigData.pdf>

⁷ <http://www.agimo.gov.au/files/2013/03/Big-Data-Strategy-Issues-Paper.doc>

⁸ http://www.iappanz.org/images/stories/2012_PA_W_IIS_and_iappANZ_Background_Paper_v2.pdf

⁹ <http://www.futuregov.asia/articles/2010/dec/08/hong-kong-launches-personalised-e-govt-portal/>

Globally, the pace of privacy reform is accelerating towards more comprehensive frameworks and regulations. Technology is also accelerating, with big data, location data and facial recognition revolutionising the way products and services are delivered online.

Online organisations should be aware that in some circumstances the collection and personalisation of customer data if mismanaged and exposed could present major risks for consumers such as increased potential for identity theft, embarrassment and financial loss.

The key for successful long term development of the internet is how to innovate and grow while addressing perceived and actual privacy concerns. And certainly there is an obligation to meet regulatory requirements. Because the internet - just like offline businesses - is a regulated place. Privacy laws are equally valid online as they are offline. Privacy regulators in some jurisdictions have released useful guidance that should be extrapolated where possible across the personalisation endeavours of companies and governments. See, for example, the Office of the Privacy Commissioner of Canada's June 2012 Policy Position on Online Behavioural Advertising.¹⁰ And the US Federal Trade Commission has published a case study on a failed Internet marketing effort.¹¹

Thus the future must be personalisation and privacy.

Conclusion

A consumer's decision to participate in an online transactions is a result of their own cost/benefit analysis. Product personalisation experiences must be clear to consumers allowing them to measure the vendor's reputation and allow them to value a more personalised service whilst contrasting privacy concerns.

The key questions every business (and privacy regulator) must ask themselves are:

Does the customer

- know what data is being collected?
- know what the data will be used for?
- know who will have access to it?
- give consent - informed consent - for it's collection?
- have the ability to opt out of such data collection and still be able to use the service?¹²

These questions are consistent with the trend towards personalisation and the notion that some of us may choose to provide information in exchange for better deals, better targeted products, and better services.

¹⁰ http://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp

¹¹ <http://business.ftc.gov/documents/someone-watch-over-me>

¹² The collection of information for fraud detection, anonymised information for account performance etc, would clearly be exempt from this.

We believe that in time Internet companies will see the value in building this trust with consumers, who will invariably see the benefits services like personalisation will bring.

If done right, personalisation will be the “Customer service” of the 21st Century.