Privacy Management, The Law and Global Business Strategies: A Case for Privacy Driven Design

Mary-Anne Williams

Innovation and Enterprise Research Laboratory
University of Technology, Sydney
Australia
Mary-Anne@TheMagicLab.org

Abstract

This paper is based on the adage that *'good privacy is good business'*. Personal information holds significant value and web based businesses often seek to monetize that value. Unlocking personal information value in web based businesses, like social networks, can lead to disclosure of private and sensitive information, and subsequent harm. Personal information management business practices are subject to privacy law, but perhaps more importantly practices that protect personal information can be a means to competitive advantage, and as a result they can form the basis of effective business strategy. We explore the underlying tension between transparency and disclosure in the privacy verses business strategy arena, and argue that the next generation of web businesses based on powerful Web 3.0 applications and services will demand a *privacy by design* approach, rather than addressing privacy concerns as an afterthought. Due to the potential power, magnitude, complexity and scope of Web 3.0 there is a need to use sophisticated technology-enabled approaches to assist users to monitor and manage personal information and its usage in a more transparent proactive fashion.

Introduction

Privacy is a social concept, and according to the UN is it a Human Right. However, there is no agreement among legal scholars or the courts on a perspicuous universal definition of privacy and attempts to capture a set of defining characteristics and properties of privacy have failed. A descriptive definition of privacy appears to be too elusive, too abstract, too multi-dimensional, too multi-granulated, too complex, too context-sensitive. McCarthy (2005) argues "It is apparent that the word 'privacy' has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts … Like the emotive word 'freedom', 'privacy' means so many different things to so many different people that it has lost any precise legal connotation that it might once have had".

Solove (2002, 2006) attempted to address the lack of agreement by advocating a novel bottom-up approach to conceptualising privacy by focusing on the specific types of disruption and the specific practices disrupted rather than looking for the common properties that all cases possess. An opponent of this idea Bruyer says that "unless a common denominator is articulated, combining conceptions simply perpetuates the piecemeal, haphazard approach to privacy that has marked the privacy landscape so far. Nor will it provide a satisfactory answer for the hard privacy cases as they occur.".

Despite the lack of a formal definition of privacy there is widespread agreement that personal information flows that respect privacy promote sustainable innovation in technology enabled services. A major challenge for legal systems around the world is to improve privacy law as a means to ensuring that poor privacy protection does not become a barrier to innovation. Particularly innovation that involves cross border information flows where information collected in one economy is processed in another. We will draw on social networks throughout because they illustrate next generation intelligent service capability and many important privacy issues which Web 2.0 and 3.0 technologies raise. In essence the root of the problem stems from the fact that these technologies are global in reach, whilst privacy and data protection regulation is local jurisdiction based law, so that local law and local legal idiosyncrasies have a global impact. The major Social Network Providers (SNPs) MySpace and Facebook are US based and essentially governed by US law.

Given the information based nature of privacy in we will focus on the protection of personal information, rather than all aspects of privacy. In June 2008 the Secretary General of the OECD stated that *"personal information is the currency of the Internet economy"*. Personal information has intrinsic value and as "owners" of that information individuals should be able to monitor and manage it as well as make informed choices and decisions about when and how to share and harvest that value.

Increasingly businesses and governments that hold personal information also have the opportunity, indeed the temptation, to unlock and harvest it too. Privacy law has an important role to play in helping to determine the balance of power between individuals and external entities like other users, businesses and governments in the management of shared personal information. Given the increasing ease with which information can be shared, the potential reach of the exchanges, the inherent difficulty of measuring the value of personal information, and the intrinsic tension between protection and exploitation of personal information it is not surprising that privacy law is currently under considerable strain. Arguably it is under global siege. Innovative information technologies and web-based services have significantly increased the richness and complexity of communication and the scope for global collaboration which in turn have lead to disruptive consumer and business behaviours that challenge existing privacy law in fundamental ways.

Privacy breaches are reported in the media almost every day and increasingly these breaches have significant and in some cases spectacular impact. Identity theft, child protection, cyberbulling, cruel pranks gone wrong, reputation damage are not only growing privacy related issues, but their impact is largely fueled by advances in web technological capabilities and the lack of globally consistent privacy protection and effective privacy enforcement law. In this paper we focus on business aspects of privacy such as target marketing rather than personal aspects like cyberbulling. Some personal aspects of privacy cut across business aspects for example how a social network website identifies potential threats like phishing or inappropriate contact with children can have a significant business impact, however we will focus on business strategies that impact privacy and personal information management directly.

In business, private information needs be to stored securely so data security is an important aspect, indeed a prerequisite, of privacy protection, however privacy protection goes beyond mere data security to encompass what and how private information is exchanged and used to provide services. Online social networking exposes many of the privacy risks and highlights the major challenges associated with maintaining privacy in an online environment. For example, Facebook continues to push privacy bounds with behavioural target marketing programs like Beacon where private purchasing information on websites beyond Facebook is used for advertising products and services to other Facebook users, e.g. friends and friends of friends. Facebook as a representative example of an SNP that continues to challenge privacy. For example, in late 2006 over 700,000 users protested about privacy issues on Facebook, in mid-2007 users complained about accounts being disabled rather than deleted, and late last year there were serious complaints about the searchability of Facebook by Google. The Age an Australian newspaper wrote after the Beacon Fiasco "After copping a barrage of criticism from users and the media, Facebook CEO Mark Zuckerberg has broken his silence and apologized for flagrantly breaching user privacy in the pursuit of profits."

Web services, innovation, business strategy, privacy and the law are not only complex activities but they are intimately and inextricably intertwined. Business strategies in the current global economy are driven by the need for high levels of strategic business innovation that deliver competitive advantage in a fiercely competitive global economy. Innovation in information technology has unleashed new and exciting business models and capabilities based on web services that further a range of social, legal, organizational, and management frontiers. Globalisation is driven by two key forces: international trade and technological advances. Contemporary businesses must be responsive to globalisation, the increasing demand for services and the changing requirements and expectations of online users. As a result innovation and business strategies are key pillars of business success in the current economic climate. Privacy is an area that continues to be profoundly impacted by globalisation, and by technological advances and innovative business practice in particular. Privacy issues and challenges loom large in the online environment and are heightened in richly connected and collaborative Web 2.0 contexts. Web 2.0 has taken the concept of a social network to stratospherical levels in terms of scale, structure and influence. As a result individuals have less control over their personal information and the way it can be accessed and used. In doing so it has not only significantly increased the potential for innovation in opportunism in the short term, but also increased the opportunity for privacy infringement. Even worse, it has heightened uncertainty and risk which could retard global development and scope for innovation in the medium and long run.

Intangible assets like brand equity and intellectual property typically contribute a significant portion of the assets in contemporary firms (Hand and Lev, 2003). Privacy is an important form of intangible asset, but unlike digital property which is essentially inexhaustible, privacy of personal information is expendable! Once private information is made public it is no longer private, and as a result it can be devalued and even worse disclosure of private information can cause significant and long term harm or damage to individuals.

Due to its cultural, social and dynamic dimensions privacy is a complex and highly contextual concept. As a result it presents significant and challenging legal issues. The objective of this paper is first to examine the complex relationship between privacy, business strategies and the law in the context of web services, second to make a case for more transparency in Web 3.0 as a means to achieving sustainable innovation, third to identify where transparency is needed and how changes in the law could help, and fourth to identify existing technology that can be used to provide the much needed assistance that will help users maintain and manage privacy in powerful and innovative ways.

We argue that appropriate and effective market equilibrium in information flow between individuals and organisations has not been achieved and that without legal

intervention it will not be achieved. A key ingredient for market efficiency is transparency, and there is a significant lack of transparency in online social networks between the major parties, namely the users and the SNPs like Facebook. SNPs hold virtually all the power in their relationship with users via User Terms of Use agreements and Privacy Policies, which they craft and modify for their own short term advantage. In other words, the lack of transparency not only helps to tip the balance of power but it biases the system to achieve an equilibrium that is disadvantageous for ordinary users' privacy. Consider for example that the SNPs know more about any given set of individuals' relationships than the individuals themselves. This places SNPs in a privileged and powerful position.

The lack of transparency stems from high levels of uncertainty, not just in the interpretation of "privacy", but even more importantly Privacy Law in a global context, and its application to the transfer, aggregation and disaggregation of user profile and activity data. SNPs use their contractual and policy power base to perform a wide range of sophisticated information gathering, processing, sharing and on-selling with complete freedom and impunity. Furthermore, in practical terms the lack of transparency and the inherent property that data tends to persist on the Web conspire to ensure that powerless users cannot make informed decisions about how their personal data is maintained and used now and in the future.

Privacy law plays a crucial and increasingly important role in innovation and the adoption of innovation in a wide range of areas, but particularly in Web 2.0 and 3.0 contexts. Privacy law that is too protective will constrain and misshape future innovation. On the other hand a laissez-faire approach to privacy law has been, and will be, a major obstacle to the widespread adoption of innovative practice and services in the long run because individuals will not engage in services where their personal information is not adequately protected. As the online environment becomes more complex and services more powerful, striking the right balance becomes harder, and there may be a tipping point where iterative changes to privacy policy and law are no longer an effective approach to evolving privacy protection and enforcement. There has been a paradigm shift in service provision since the advent of Web 2.0 which may require changes in the legal system of equal scope and magnitude. In the case of privacy protection the long term benefits of introducing disruptive legal changes may outweigh the short term cost. The idea being that more comprehensive redesign of laws has a better chance of creating a conducive environment for innovation in the long term than tweaking and fragmenting existing laws and introducing additional laws.

Transparency will help to ensure that the objectives and expectations of users and advertisers can be matched more effectively. It is in the user's interest to see advertisements that are relevant but not at the cost of discriminant and indiscriminant information leaks and privacy invasion. Web 3.0 providers (W3Ps) need to be cognizant of how their tools and services will operate and what privacy controls they will have in place. If a firm promotes a new Web 3.0 service and targets potential customers using information that the user has designated as private, or if the firm sells access to personal information that can identify individuals directly or indirectly, then the user should be made aware, i.e. notified, and provide consent.

In order to attain sustainable business success W3Ps need to create a trusted business environment where users are willing to share information. There is a strong positive relationship between trust of business and competitive advantage (Barney *et al*, 1994). Trust involves sharing a common understanding of intent and expectations regarding shared information usage. It seems rather obvious that a business like Facebook which was valued at US$15Billion last year could and should invest in better privacy protection in order to achieve sustained success, instead of shirking responsibility at the expense of its 60 million users. Perhaps its growth stagnation, in the US in particular, is a reflection of its denial of privacy and privacy concerns. Recent events in the financial markets highlight how things can go wrong when trust in the marketplace is lost or undermined.

Improving transparency is part of the solution, however identifying what information and processes are transparent and how is nontrivial because making some information gathering and processing procedures publically available can be used for criminal activity e.g. information about counter measures may assist spammers, strangers approach children, and users exploit other users. However it seems reasonable for W3Ps to highlight the need to review and understand privacy policies, to offer real choice in privacy settings, to teach users how to review and adjust their privacy settings, to alert users to changes in policies that are potentially privacy infringing activities, to notify users about clickstream information being captured and shared, to allow users to all traces of their personal information including interactions with others (Gilbertson, 2006). Users should be made aware of who their personal information is shared with, how and when., e.g. Facebook declares that it collects *"information about you from other sources, such as newspapers, blogs, instant message services."* but it does not provide any specific information about the nature of the information collected.

Some important concepts in the Web 2.0 and 3.0 privacy debate are user choices, information flows, information transaction/exchange, trust, control and influence. Personal information flows are a basic activity in Web 2.0 and 3.0; they can be used to define information processing of personal information including information exchange, aggregation and disaggregation. Trust, like privacy, is a multi-dimensional concept whose meaning is dependent on culture and context. Trust between users and service provides plays an important role in Web 2.0 and 3.0. It influences what, how and why specific information is exchanged, particularly in social networks between "friends" and "friends of friends". Trust is difficult to describe and define because of its complex character but

also because of the way it is used. It can be conceived as a measure of confidence in the future behaviour (Barney, 1994). In particular, it is often used to help determine the quality and credibility of information and to determine what and how specific information can be propagated with in a social network. As a result trust is used as a mechanism for controlling and influencing information propagation within a social network. Social networks can be analysed and understood from two perspectives: the user profile information view like name, age etc, and at the network view of connections and information activity flows. Distinguishing these views is particularly important for understanding the legal aspects of social networks.

In addition, to the fact that the law lags technological advances and is typically bound by jurisdiction and there is significant variation across the globe in privacy law, and the major divide between US and EU law in particular. Furthermore, most Internet users reside in developing countries where privacy and other law is emerging. It is for this reason that now could be a good time to consider sweeping developments in privacy law and global adoption of privacy management strategies.

Business Strategies

The web has been available to the general public for over a decade and it has evolved through three major phases. The first phase can be classified as *mass consumerisation* where businesses like Amazon collected consumer profile data, viewing activity and transaction based information. This early phase was marked by widespread disintermediation, and privacy issues mainly concerned the secure capture, authentication, transfer, storage of and access to the customer personal transaction information. The second phase, Web 2.0, took online interaction to the next level creating the era of *mass prosumerism* which allowed consumers to also produce content and to create value for online business, e.g. Trip-Advisor. In the age of prosumerism privacy issues arise around storage and protection of personal information, but additionally the content of user postings. We are now embarking on the third phase, Web 3.0, *mass socialisation services* where people share rich and significant amounts of personal information like opinions and photos on an unprecedented scale, and indirectly through their online behaviour. This phase is just beginning and the predictions of where it might go tend to suggest widespread adoption of intelligent technologies such as the Semantic Web, Data Mining, and Intelligent Geo-location services.

Social networking is the most rapidly growing area of current Web 2.0 activity where individuals create online profiles, make connections with others and share information including personal information. The Social Software Weblog has classified several hundred social networking sites into nine categories. Some specific emerging business models based on social network strategies include: Appvertising: Buddymedia, Social Media, RockYou; SocialCommerce: Paypal, Social Cash, QQ Com (China); Business Social Network: LinkedIn – exchange knowledge, opportunity and advice which is designed for the business professional.

The Chi.mp is a new SNP, currently in alpha release, that is trying to promote interoperability among the SNP platforms. In fact, in terms of business strategy interoperability is central to Chi.mp's competitive advantage. The idea is that the Chi.mp platform in contrast to other social networks which operate as a standalone closed network (so-called walled gardens), notwithstanding programs like Beacon which are built on specific business partnerships, rather than being part of the basic infrastructure. Chi.mp is a good example of the next generation social network. It lets you connect your profile to others in a free and open network, instead of being locked inside, as it puts it, a walled garden. Chi.mp makes the point that it is important for networks to interoperate and they illustrate in the statement "We wouldn't own a cellphone that would only allow us to call people on the same network, we should demand the same freedom with our identity on the web." Chi.mp provides a centralised digital identity management system where users can have more than one identity that the user can control. It uses OpenID to log in to external website. Realistically people do not have a single identity, we like to have more than one persona. In some contexts a person may wish to be perceived as a parent, in others a child, a professional, a sports player, etc. Chi.mp users can determine what others can view and access. It allows the user to tag relationships and as result users have considerable control and flexibility in choosing what profile to show to whom.

Privacy and Privacy Law

If personal information is the currency of the Internet as the Secretary General of the OECD recently stated, then it is important to safeguard it and keep it safe, but how safe and safe in what sense? Taking this analogy to the next level consider the hypothetical notion of a Privacy Bank, and ask what kinds of services would we expect such a bank to provide. Some candidates for a barebones management service might allow the "owners" of the personal information to inspect, change, evaluate, and exchange it. More sophisticated services might include facilities for planning, commercialising and monetising. There are many similarities between money and personal information as a currency in the respective markets such as its ability to be reinvested and lost. The key difference is that personal information is tied to particular people in a way that money is not, and an individual may wish to keep knowledge about the personal information limited to a small trusted group and not allow on-selling. It is this difference that would have the most impact on services offered by a Privacy Bank because when the bank lends its resources to others it would need to act responsibly by providing appropriate levels of protection in line with individuals' expectations. Protection comes at a cost, there would be transaction and administration charges. Clearly it is in an individual personal information lenders

interest to manage their personal information portfolio with that in mind, so that unduly restrictive protection was not provided to personal information that did not require high levels of protection, because it is not sensitive or because it is already completely or partially publically available. Banks offer standard management accounts for financial resources, so what would be stopping a privacy bank offering attractive standard accounts for personal information?

Just as banks act as an intermediary between providers of funds and consumers of funds, why not a privacy bank that acts as a mediator which could aggregate content across its customers under strict accountability requirements. Customers could choose to use the bank services they wanted. There are parallels between money management without banks and current privacy management. Imagine if there were no banks to obtain interest from and no banks to gain loans from, but just a market in which borrowers and lenders had to locate each other and negotiate exchanges. It would result in chaos, much like the privacy management space today. Individuals have a valuable asset, personal information, but limited ways to manage and exploit it. Given the potential for developing competitive advantage it would seem that personal information management based on Semantic Web technologies could be lucrative.

Social networks like Facebook and MySpace continue to face security and privacy related issues as functional capabilities expand and social interactions within the community become more complex. The Beacon program is an opt-out program which tracks user activity long after users have logged off the Facebook website and even when users have elected to not display their activities to Facebook friends clearly challenges privacy. It is a form of covert surveillance. User activities are tracked on Facebook partner sites like Blockbuster and made accessible to Facebook who then broadcast those activities to the user's friends on Facebook.

Some social networking sites have had to shut down due to privacy concerns, e.g. the highly innovative Semantic Web powered social network *Plink* (Golbeck, 2005). These concerns involved access from outside the network and the aggregation of personal information via advanced technology and business intelligence techniques. This example provides compelling evidence for the claim that short-sighted privacy protection in technology-enabled innovation does not lead to sustained rewards and the need to protect and enforce privacy only become more acute because technological advances show no sign of decelerating or abating.

According to Abrams (2006) "Privacy law is culturally based. Privacy is considered a fundamental human right in Europe, highly regarded with pragmatic interest in the United States, and is only beginning to emerge as a topic in Asia. What works in one country or region doesn't always work in the other."

Privacy is a relatively modern concept but protected differently across the various jurisdictions because of cultural predilections and historical events. Major theoretical and practical differences exist between EU law and US law (Whitman, 2004), in particular. In Europe privacy related law tends to focus on restricting private business practice, whilst in the US it focuses on government powers. There are few legal constraints on social network businesses like Facebook in the US. In Europe countries like France, Germany and the UK as members of the European Convention on Human Rights must respect Article 8 ECHR, which guarantees a "right to respect for privacy and family life". In the Asia organisations like APEC (Crompton, 2008) which includes member countries USA, Canada, Japan, Korea, Hong Kong, Australia, New Zealand, Taiwan, Russia with privacy law with enforcement, countries with minimal and evolving privacy law China, Singapore, Malaysia, Thailand, Mexico, and those where privacy is not high on the political agenda Chile, Indonesia, Vietnam, Malaysia. India a key emerging economy is not a member of APEC.

In the UK there is no tort law doctrine that gives rise to a right to privacy, e.g. *Kaye v. Robertson* [1991] FSR 62 and *Wainwright v. Home Office* [2003] UKHL 53. The European Union Directive on Data Protection of 1995 mandated that each EU nation pass a national privacy law and create a Data Protection Authority to protect and enforce privacy. In the EU personal information cannot be collected without the individual's permission, individuals have the right to review the data and correct inaccuracies, firms that process information must register their activities with the government, employers cannot read employee's private e-mail, and personal information cannot be shared by companies or across borders without express permission from the data subject.

The difference between U.S. and EU attitudes towards privacy laws stems from their divergent views and trust of government verses corporations. In the U.S the Federal Trade Commission seldom acts against U.S. firms, however Data Protection Authorities in Europe monitor corporate behaviour carefully. Privacy laws and consumer concerns can and have had dramatic effects on business, especially cross border business. Increased concern for terrorist activities has lead to a number of breaches where the U.S. government acquired information contrary to several European countries law, e.g. airline passengers. Privacy law in the US is deemed to be weak in global terms with respect to placing constraints of business practice and it is fragmented across a wide range of law and policy areas, e.g. the Fair Credit Reporting Act 1970 and amendments, Privacy Act 1974, Family Educational Rights and Privacy Act 1974, Health Insurance Portability and Accountability Act (HIPAA) 1996, Children's Online Privacy Protection Act 1998, Gramm-Leach-Bliley Act 1999 for privacy in the finance industry, and many Federal laws. In addition, most states have laws that impact on privacy. Furthermore, differences between Europe and the U.S. approach to privacy protection and enforcement has had significant impact on cross border business because EU's Data Protection Directive can be used to ban the transfer of data to countries without comprehensive

privacy protection laws. It is widely accepted that the US has weak privacy protection laws and as a result had to be granted special dispensation a "safe harbor" agreement which promises privacy controls on EU data that flows into the U.S. Clearly this is a stop-gap measure and not an adequate and sustainable solution. The major differences in EU and US privacy related law as applied to Web applications are summarized in Standler (1998).

U.S. privacy law mainly protects the liberty of the individual from government agencies and grant protection at home. European and U.S. laws also diverge widely on limiting press freedoms, with U.S. courts granting boarder flexibility over publication of personal information. On the hand, the US has quirky strict laws across it states, and narrow historically motivated federal laws such as the 1988 Video Privacy Protection Act created in response to a newspaper publishing the video rental records of Judge Robert Bork during Supreme Court hearings concerning his nomination.

Privacy law in Web 2.0 services such as social networks has tended to focus on the information life cycle of collection, accuracy, use, and security, as well as the need for transparency and user control of personal information. The debate revolves around consent, notice, necessary collection, SNP and third party usage, and user access, correction and deletion.

Consent, Choice and Control

Greenleaf (2003) discusses four critical aspects in determining consent: (i) the context in which the consent is sought, (ii) whether there is informed consent, (iii) whether the consent is voluntary, and (iv) whether the individual's option to consent to one purpose is freely available and not bundled with other purposes.

Consent should be informed and freely provided. It is unclear whether Web 2.0 services like social networking websites obtain consent, since the purpose provided for collection is often not only general but sweeping. Moreover in most cases it could hardly be described as informed, since even the SNP does not know what they might do with the personal information they collect, and it is questionable if the information is given freely because users are not provided with a choices once they start interacting with the system, for example it is not uncommon for changes that impact consent to take place. The introduction of the Beacon program by Facebook on the basis of an opt-out without any notification that it was introduced and the implications of its introduction is a prime example. So in social networks it seems to be that users do not give unambiguous consent, indeed they even lack a basic awareness of how their personal information is used.

The EU Directive requires that "*the data subject has unambiguously given his consent*" (Art. 7(a)) as one of the bases for any processing of personal information. The operative word is unambiguous, so if consent is implied it must be unambiguously implied too. Unambiguous consent is difficult to establish in a Web 2.0 service context for each piece if information collected. Failure to opt out is related to consent being implied. For example, if a person has already provided personal information, but is only then presented with an opt-out notice concerning additional uses of the information, that is not consent as determined in *Australian Communications and Media Authority v Clarity 1 Pty Ltd* (2006) 150 FCR 494 – a *Spam Act* 2003 .

Greenleaf emphasizes that the failure to opt out is not by itself consent! Consent for uses and disclosures verses acknowledgement to conditions such as notification. These are often confused and need to be distinguished according to Greenleaf. SNPs regularly bundle consent as a means to reduce the business burden in terms of cost and risk. Furthermore, they do not know themselves how they will use the personal information they collect in the future. The practice of seeking consent for multiple uses and/or disclosures at the same time is not acceptable when the potential for privacy invasion is high or worse unknown. Individuals are given no choice as to the particular uses or disclosures to which they are consenting. Users are presented with a limited choice, and it raises the questions as to whether consent can be construed as freely given.

Bundled consent can undermine privacy and lead to breaches. Businesses typically employ bundled consent practice for reasons of efficiency and cost reduction. There need to be clearer guidelines that limit bundled consent. Getting the limits right is also in all the stakeholders long term interest since having to give consent for each information flow or exchange would reduce productivity for all parties. The upshot is that W3Ps should give clear guidelines that state when data users are allowed to rely on consent obtained in this way and conversely, the extent to which individuals must be given separate opportunities to consent to different uses/disclosures.

Privacy Management Issues and Tools

Protecting privacy is big business, particularly in the US where privacy related law as applied to business is weak. For example, *ReputationDefender* specialises in protecting and enforcing the privacy and reputation of its clients. It does so proactively by constantly scouring the web for personal information. There are a wide range of technological tools that can be used to help protect and manage privacy. They include generic tools and approaches like autonomous software agents, customised software like *PrivaWorks*, IT standards CLPC IP31, and the Enterprise Privacy Authorization Language (EPAL) which is a formal language that allows developers to specify fine-grained enterprise privacy policies.

The major disadvantage of being trapped in the walled gardens of Web 2.0 is the lack of privacy management tools choices. At present the only tools available for users to manage their private information in social networks like MySpace and Facebook are seriously limited and fall short in several key areas. For example, removing personal information is problematic and since SNPs have an interest in maintaining removed users nodes

within the network in order to preserve the network linkages, user information tends to persist.

In social networks users are typically required to provide personal profile information to create an account and then they have control over the information that they provide to limited extent. Managing profile information is relatively straight forward; profile information in most social networks is not verified and so need not actually be accurate. In terms of privacy the real challenge lies in the rich information that the user provides about himself, his friends, and their preferences, interests, behaviours, and actions explicitly and implicitly. Moreover, this information often has complex relationship with other users information, and this relationships is not managed by individual users but by the SNPs. Most value in a social network is in the relationships not the profile nodes.

In summary the key challenges for privacy management systems are: determining and managing private (personal protectable) information over time, determining consent, creating suitable contracts/licenses, determining breaches, notification, improperly repurposing content, and handling context.

Building sophisticated services that can reason about "permission" and "obligation" for privacy (Kagal and Finin, 1992), "*A* has *permission to access* information *i about person x*", "*A* has *permission to transfer access* of information *i about person x*", "A has an *obligation to protect* information *i about person x*", and to ask queries like "Can I tell *Z* about *i*" , "Does *A* know *i*". Could prove to be a useful direction to explore.

Users have high levels of engagement if they trust their partners, have sufficient information to make informed decisions, and feel empowered. Empowered users are more open to innovation adoption in Web 2.0 because they are able to make their own choices about the availability of their information." Trust plays an important role in user adoption of innovative technologies and new business models. Jutla *et al.* (2004) provide empirical results that quantitatively show that user intervention tools for privacy significantly contribute towards online trust. They measure five user intervention mechanisms for trust: P3P, cookie crushers, encryption, pseudonymizing, and anonymizing tools

Challenges Ahead

The web is evolving rapidly and becoming increasingly rich and complex. We all have a digital footprint that Web 2.0 and Web 3.0 applications can discover and exploit, e.g. behavioural targeting of users for products and services. The forms of exploitation can lead to the disclosure of personal information, the invasion of privacy and subsequent harm.

In February this year Justice Michael Kirby of the High Court of Australia said that "technology will outpace in its capacity, the imagination of even the most clever law makers". Clearly, the law has little to offer and technological solutions are needed. In a similar vein in Europe the Information Commissioner in the UK has recognised the impact of technology on law making where he stated that he "believes that the time has now come to start a new debate. This recognises the pace of technological change ... [and] .. a growing feeling that the [EU] Directive is becoming increasingly out-dated ...".

The underlying nature of the web and how it is used has changed dramatically over the last decade profoundly effecting privacy and personal information management. It has become more densely connected and due to advances in technology-enabled innovation rich and complex relationships between people and organisations can be supported. This development is a major shift from the one-to-one relationships of the past to the potential many to many multiple layered relationships of the future.

In a Web 3.0 environment protecting and enforcing privacy will come at a major cost to business and a lack of privacy creates risk for users. The stakeholders in the privacy in the Web 3.0 debate are business, privacy advocates, consumers, and regulators. A sustainable approach to improve privacy protection must balance the cost and risk profiles across the stakeholders. A shift in the risk burden in from users to Web 3.0 business requires more accountability and transparency on the business side but the business rewards are potentially huge.

As noted earlier an unambiguous definition of privacy is not available. Furthermore, there is a school of thought that takes the famous statement of Sun's Scott McNally "There is no privacy, get used to it" to a new level by arguing that a lack of privacy is good for society because it creates a culture of openness which over time would give rise to a society with reduced anxiety, fear and discrimination. This school argues that openness makes it harder to deceive and harder to hide from the truth and that positive ramifications follow. The downside is that without any form of privacy, personal information could and would be used for harmful purposes. Paradoxically openness can lead to both positive and negative effects; unfortunately acquisition of personal information about people can empower those who would want to cause harm.

University of Queensland law professor Jim Allan makes a crucial point, he argues that "In any contest between privacy and free speech, I think we should err on the side of free speech: allowing people to speak their minds has very good consequences,… Privacy laws tend to kick in when people have said things that are true. It's a fairly dangerous thing to prevent people saying things that are true ... My view is that we live with the law of defamation: you say something untrue and you pay the consequences, but if it's embarrassing, so what?"

There are major advantages in pursuing a better global regulatory environment because it will result in sustained innovation, easy, effective engagement with customers and business in other economies, and release of economic value.

What is good for Web 3.0 innovation is the free flow of personal information in a way that respects privacy. A major barrier to achieving the free flow of

personal information is the privacy issues which are raised in cross jurisdiction data flows where information collected in one economy is processed in another. In the cross border online personal information processing context technological solutions is needed that respect and propagate the original privacy promise as determined by the information sources jurisdiction law, company privacy policy and other undertakings, consumer choices.

Trust plays an important role in protecting privacy and without trust consumers avoid engagement, they minimise or falsify responses, and as result business opportunities are missed, and innovation suffers in the long run. If users do not trust a specific business to respect and protect their privacy then they will avoid providing personal information or falsify the information they provide.

Given that the most popular SNPs are based in the US, the best hope of improving privacy in Web 3.0 is to raise the bar on privacy related law in the US.

Future Developments in Global Privacy Law

Privacy protection and enforcement are global problems which are currently addressed through a complex, incomplete, uncertainty and changing mosaic of law. This is not a desirable situation given the negative impact poor privacy and personal information management has on innovation and business strategies.

There is a global trend towards a principles based approach to protecting privacy as a means to future proof the law in a wide range of jurisdictions. According to the Optus submission to the recent Australian Law Reform Commission privacy review '[t]he current principles based, technology neutral regime provides a powerful framework on which to base privacy requirements when assessing new and emerging technology'.

Given the difficulty in anticipating technological advances and their impact on innovation, privacy law should be technology neutral. US law stands out as a laggard in the evolution of privacy law relative to the EU and emerging developments in Asia. Given how far behind the rest of the developed world it is in protecting individuals personal information with respect to business practices in the private sector, it needs to revolutionize it privacy law just to catch up. Most of the Web 2.0 and potential Web 3.0 services are based in the US and as a result long term innovation could be compromised.

Google is aware of the need for change and has advocated the creation of a global standard for handling private consumer information and put forward the useful idea of including a harm condition so that remedies can take the degree of harm into condition. But what is really needed is better regulation, not more regulation.

Future Developments in Global Privacy Governance

According to Harriet Pearson (2008) the Chief Privacy Officer at IBM privacy has become a source of anxiety and corporate concern. Consumers are concerned and sometimes anxious that personal information can be exchanged, bought or sold for secondary use without their knowledge or consent. Furthermore, they are concerned about identity fraud, use of personal information on the internet, businesses sending personal information overseas for processing and the use of personal information for marketing.

Privacy protection and enforcement are not only a cultural issue in society, they are a corporate culture issue. Firms who understand the importance of maintaining their customers privacy in return for their loyalty have always lasted longer in the market place. Many Fortune 500 firms have developed internal Privacy Governance Frameworks which typically includes a high level policy, standard operating procedures, a range of performance measures, assurance, compliance and best practices.

Future Technology Challenges for Privacy

The main challenge facing technological approaches is that privacy is a local phenomena while the processing of personal information is global. The debate about privacy and the future of technology centers around the exploitation and potential for privacy violations versus enhanced customer service.

Personal information is defined extremely narrowly by some Web 2.0 services. For example on the social network Twine the term "personal information" means "information that specifically identifies an individual (such as a name, address, telephone number, mobile number, e-mail address, or other account number), and information about that individual's location or activities, such as information about his or her use of the Site, when directly linked to personally identifiable information." . This definition does not include a users network connections and activity which are the most value information in a social network. Facebook does not provide convincing or comforting support that it protects personal information "You post User Content …on the Site at your own risk…. we cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons."

Major technology-enabled innovation trends that will significantly impact privacy and personal information management include data fusion, cloud computing, geo-location based services, and semantic web technologies as they become more mainstream across a wide class of applications from enterprise systems to social networks. According to the Merrill Lynch May 2008 Report (FutureLab 2008) the annual global market for cloud computing will reach $95 billion over the next five years, and 12% of the worldwide software market will involve cloud computing. Semantic web technologies offer extraordinary promise for social networks, their main failing to date is that they do not design for privacy. For example, one of the most innovative exciting social networks was Plink which had to close down due to the privacy issues its highly sophisticated engine generated. Plinks downfall clearly highlights the need for develops to take privacy more

seriously by making its protection and enforcement a high priority in systems requirements.

Geo-location detection services are a growing application area with vast potential. They enable the location of individuals to be determined in real time and at the same time generate rich personal information about the physical location and movements. Data mining, matching and fusing techniques can be used to derive substantial personal information about individuals like consumer preferences and behaviours.

The European Union Directive on privacy and electronic communications deals with 'location data' which they define as 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service'. The EU Directive prohibits the processing of location data that has not been anonymized without the consent of the user of the service, and before seeking consent it requires businesses to inform users of the type of location data that will be gathered and process, as well as the purpose and duration of the processing. Businesses must also inform the user if the data will be transmitted to a third party. These kinds of legal requirements are lacking in US law.

Intelligent data-matching, data-mining and data fusion practices involving personal information raise a number of privacy concerns, however appervising firms are using these techniques more and more in social networks looking for nuggets of value in user s personal information to exploit.

In summary we agree with Richard Purcell, the former CPO for Microsoft who stated "Respect customer information for what it is: a key asset for business success. Protect it with the same care you give trade secrets.". Furthermore, just like trade secrets, protecting personal information will lend to significant competitive advantage because it helps to create a trusted business environment. In this paper we argued that the next generation of web services based on powerful Web 3.0 technologies should take a *privacy by design* approach, rather than addressing privacy concerns as an afterthought.

References

Abrams,M. 2006. 'Privacy, Security and Economic Growth in an Emerging Digital Economy', Privacy Symposium, Institute of Law China Acad of Social Science.

Barney, J.B. & Hansen, M.H. 1994. Trustworthiness as a Source of Competitive Advantage. *Strategic Management Journal*, 15, 175-190.

Bruyer, R., 2006. 'Privacy: A Review and Critique of the Literature', 43 *Alberta Law Review* 553, 576.

Bennet C. and Raab, C. 2006 *The Governance of Privacy Policy Instruments in Global Perspective,* MIT Press.

Breach Reports, http://www.nymity.com/BreachReports.asp

Cockfield, A. 2007. 'Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies', 40(1) *University of British Columbia Law Review* 41.

M Crompton, The APEC Privacy Framework *Creating Trust in developing Cross-Border Privacy Rules: A Progress Report, http://www.iispartners.com/apec8march.pdf*

Engelmore, R., and Morgan, A. eds. 1986. *Blackboard Systems.* Reading, Mass.: Addison-Wesley.

Dwyer , C. , Hiltz, S., Passerini, K., Trust and privacy concern within social networking site: A comparison of Facebook and MySpace, AMCIS2007

FutureLab. 2008. http://blog.futurelab.net/2008/05/

Gerstein, S. 1984. Intimacy and privacy. In F. D. Schoeman, editor, Philosophical Dimensions of Privacy: An Anthology. Cambridge University Press, UK.

Gilbertson, S. Delete your bad web reputation, *Wired*, 2006 www.wired.com/science/discoveries/news/2006/11/72063

Golbeck, J. 2005. Social Networks, Privacy, and the Semantic Web, Tuesday October 11, 2005 http://www.oreillynet.com/ xml/blog/2005/10/social_networks_privacy_and_th.html

Greenleaf, G. (2003) APEC privacy principles: More Lite with every version http://www2.austlii.edu.au/ ~graham /publications /2003/APECv5_article.html <viewed 7 Aug 08>

Hand, J. and Lev, B. (Eds), (2003) Intangible Assets: Values, Measures and Risks, Oxford University Press.

Jutla, D.N.; Kelloway, E.K.; Saifi, S. Evaluation of user intervention mechanisms for privacy on SME online trust, CEC 2004. Proceedings. IEEE International Conference on eCommerce Volume , Issue , 6-9 July 2004, 281 – 288

Kagal, L. and Finin, T. 1992. Modeling Conversation Policies using Permissions and Obligations http://ebiquity .umbc.edu /_file_directory_/papers/92.pdf <viewed 7 August, 2008>

Lohr, S. "Computing, 2016: What Won't Be Possible?" New York Times, October 31, 2006.

McCarthy, J. 2005. *The Rights of Publicity and Privacy.*

OECD Ministerial Meeting on the Future of the Internet Economy, June 2008: Shaping Policies for Creativity, Confidence and Convergence in the Digital World www.oecd.org/ FutureInternet <viewed 7/9/ 2008>

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data .oecd.org/document /18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

Pearson,H. 2008 Privacy is good for Business www-03.ibm.com /innovation/us/customerloyalty/harriet_pearson_inteview.shtml

Plink http://web.archive.org/web/20040412114701/beta.plink.org

Privacy Law in the US www.rbs2.com/privacy.htm

Privacy (Stanford Encyclopedia of Philosophy) http://plato. stanford.edu/entries/privacy/

Prosser, D. 1960 'Privacy' 48 *California Law Review* 383

Solove, D. 2006. 'A Taxonomy of Privacy' 154(3) *University of Pennsylvania Law Review* 477, 485– 486.

Solove, D. 2002 'Conceptualizing Privacy', 90 *California Law Review* 1087.

Standler, R. 1998, Privacy Law in the US, last revision, Accessed in August 10, 2008 [http://www.rbs2.com /privacy.htm]

Warren and Brandeis, 'Right to Privacy' (1890) 4 *Harvard Law Review* 193

Westin, A. 1967, *Privacy and Freedom*, New York: Atheneum

Whitman, J. 2004. "The Two Western Cultures of Privacy: Dignity versus Liberty." Yale Law Journal, Vol. 113 April.