IDIS (2010) 3:319–341
DOI 10.1007/s12394-010-0057-8

Layering privacy on operating systems, social networks, and other platforms by design

Dawn N. Jutla

Received: 30 October 2009 / Accepted: 12 April 2010 / Published online: 18 May 2010

Abstract Pervasive, easy-to-use privacy services are keys to enabling users to maintain control of their private data in the online environment. This paper proposes (1) an online privacy lifecycle from the user perspective that drives and categorizes the development of these services, (2) a layered platform design solution for online privacy, (3) the evolution of the PeCAN (Personal Context Agent Networking) architecture to a platform for pervasively providing multiple contexts for user privacy preferences and online informational privacy services, and (4) use of platform network effects for increasing wide-scale user adoption of privacy services. One implication of this paper's concepts is that platform-mediated networks, which are reportedly the vehicles for most of the revenue earned by 60 of the world's largest companies, and other platforms that commonly host millions of users, will not have to individually reinvent and manage sophisticated user services for privacy protection since universal privacy platforms can be layered on them in future.

Keywords Online privacy platform · P3P · PeCAN platform · Social networking · User adoption of technologies · Web privacy services · Identity protection

Introduction

Privacy advocates are working with modern and innovative environments in which operations take place that are beyond the citizen's control, and/or do not yet fall within the realms of governance. One such environment is the global Internet, where experimentation with business models is rampant, the combinations of multi-cultural approaches and infrastructure readiness is uneven on a per-country basis, and users are mass-adopting new and disruptive technologies in the shortest cycle times ever

D. N. Jutla (✉)
Department of Finance, Information Systems, and Management Science, Sobey School of Business, Saint Mary's University, Halifax, NS, Canada
e-mail: dawn.jutla@smu.ca

witnessed in world history. To add to this dynamic picture of progress are uncertain economics, as at the end of the first decade of the twenty-first century, major and minor economies are in recession, or declaring the end of it with predictions of sluggish growth for coming years. However, interestingly, even in these times, firms on the Internet, particularly social networking platforms, have experienced huge user growth. Countries, rich and poor, have significant percentages of young people online.

In October 2009, the social networking platform Facebook™ had over 300 million active users, and one million developers and entrepreneurs from over 180 countries (Facebook Statistics 2009). Its fastest growing demographic segment was approximately 35+ years old, whereas in September 2008, Facebook claimed 200 million active users and its fastest growing demographic was the 25+ age group.

In 2010, Facebook supports over 400 million active users. Moreover, seventy percent of Facebook users are outside of the US. Clearly, users greatly value the functionalities offered by such vehicles of worldwide, culture-crossing social innovation. Online social networks (OSNs) are now in a position to create and sustain new and old social norms for generations of users. The balance between personal branding and privacy is being tested and socialized.

In the OSN environment, one question that arises is whether users care about privacy and its long-held status as a social norm. OSNs' experiences with user outrage and legal action over previous launches of privacy-invasive services indicate that the answer is affirmative. One such experience was recorded when Facebook launched its News Feed service from the Facebook Home Page in September 2006. Initially the service was opt-out and it automatically displayed all rich social information regarding recent activities of friends to other friends. Hostile user reaction emerged to having user information and interactions monitored and pushed to friends. Users formed groups, such as Students against Facebook, to speak out about the service's privacy problem. Facebook immediately responded to its users' outcry, and added privacy controls to allow users to decide what information they would allow to be pushed to others. Facebook's CEO also publicly apologized for his company's mistakes concerning privacy in the OSN.

Surprisingly, given recent company experience with user privacy, but not so surprising from a profit or business experiment perspective, one year later Facebook launched a privacy-infringing service called Beacon. Coupled with Facebook Ads, the Beacon service widened the scope to communicating user data from external parties, namely ad sponsors (i.e. companies) to the user's friends. In effect, information regarding products that a user purchased, or commented on, from a partnering company's site would be pushed to the user's Facebook friends without explicit user permission. Additionally, many users were not informed about the program beforehand. This privacy violation was larger than the last and users escalated their outrage to a class action suit that was settled in Sept 2009, the same month that Facebook reported being cash flow positive for the first time. As part of the legal settlement, Facebook agreed to shut off its Beacon service and pay USD 9.5 Million to fund a privacy and online safety foundation. Again, the CEO of Facebook publicly apologized, the issue subsided, and the OSN continued to grow rapidly. By now the 6-year old OSN was exhibiting a strategy of launching for profit services that shared users' data with many parties, and when or if users objected

about the company's handling of their private data, the company reacted by making amends and seeking forgiveness from its users.

Meanwhile in 2008, on the international scene, the Canadian Privacy Commissioner, Jennifer Stoddard launched a yearlong investigation on Facebook's privacy practices, after a number of Ottawa University Law students and the Canadian Internet Policy and Public Interest Clinic filed a complaint about Facebook privacy practices and potential violations. Her investigation's 2009 conclusions cited that Facebook needed to improve its privacy practices by improving its explanations around user privacy, restricting unnecessary access of user information to application developers, and not retaining user personal information after her/his account is deleted. Again, Facebook cooperated with the Privacy Commissioner's Office to address its concerns. However, in 2010, the Commissioner started a further investigation into Facebook's new privacy policies, after a Canadian user filed a complaint alleging that Facebook's December 2009 default settings made his information more available to others.

Understandably, unsuspecting users do not immediately think of privacy issues when they join an OSN to network with friends and acquaintances. However when users notice infringement on their personal space, privacy is clearly important to them. Also apparent is the tension between user privacy and the OSNs business model. Again using Facebook as a good example, we see the bold 2008 launch of Facebook Connect. This time Facebook could give rich user data, including but not limited to profile information, social graph information such as Facebook IDs of all friends and spouse, number of wall posts and notes, photographs, tags etc., to companies that participated in Facebook Connect. One key difference in this service's launch was that Facebook gave privacy settings to allow users to control what information, if any, is provided to the companies. Due to such organizational learning, Facebook is currently a leader in the OSN space not only for its functional value but also for the privacy controls provided to users.

As of March 2010, 80,000 web sites were participants and formed a chargeable customer group within Facebook Connect. In turn, Facebook users enjoyed the easy functionality of single sign-on using their Facebook authentication credentials to log into other web sites, the transfer of their own and friends' information from the sites back to Facebook, and the easy viewing of their friends' related information from their interactions with the external company sites. With Facebook Connect, the OSN is moving to a single portal from which users will conduct everyday tasks such as bank, register for courses, pay bills, and buy goods.

Given the rich personal data exchange, a current issue that worries privacy advocates is whether users are actively setting their privacy preferences on OSNs. Ethical business practices would guide OSNs into caring about user education in the privacy space. Due to the aggressive user growth rate, the importance of branding and reputation, and previous brushes with users' outrage over their privacy infringement, platform sponsors and providers of OSNs should be receptive to their users, privacy associations, privacy commissioners, and governments' advocacy, and be willing to pay close attention to their users' needs around handling of their private data. Moreover, on the flipside, these social networking platforms present an inexpensive and effective opportunity for national privacy advocates to reach out to

hundreds of millions of their citizens to increase user's awareness and education around privacy. Such user education, at a minimum, influences how users share, protect, and hence control their private information, and informs users how to avert or detect poor handling of private data, and to avert and/or resolve private data handling disputes in future.

This paper presents a novel proposal to suggest that privacy platforms for awareness and education, and aggregation of privacy technologies for users to protect their privacy, detect privacy violations, and resolve privacy disputes are the way to go in the future. This proposal is a large step forward in comparison to the loose bunch of point technologies that are available now. For privacy platforms to be workable, they need to be sandwiched between other platforms such as operating systems, mobile devices, and social networking platforms. In effect, this paper's proposal and design that layers privacy platforms onto operating system and social networking platforms may realize the opportunity to mature the services for the user privacy lifecycle universally across platforms and hence help billions of citizens to become more privacy-aware and in control.

The user's online privacy life cycle

In the last decade, several organizations and researchers attempted to classify privacy technologies. Best known are the Organization for Economic Co-operation and Development's (OECD 2002) and Olivier's (2003) single-level classification systems. The OECD classification supports four categories: personal privacy enhancing, web-based, information brokers, and network-based as shown in Table 1. Unfortunately, some of the OECD categories greatly overlap. For instance, personal privacy enhancing technologies and information brokers are web based. A better classification is Olivier's (2003) as shown in Table 2. The computer science researcher presents five categories according to the purpose of stakeholder usage: private communication, anonymity, personal control, organizational safeguards, and inference control.

This paper proposes a higher-level classification system, according to user behaviour within a privacy lifecycle. This lifecycle system is multiple-level (Jutla et al. 2010) where each phase of the lifecycle presents itself for further sub-classification. However, due to space limitations, this paper describes only the top-level of the privacy lifecycle classification.

Table 1 OECD classification of privacy technologies

Privacy technology category	Examples
Personal Privacy Enhancing	Cookie managers or blockers, ad blockers, encryption software
Web-based	Anonymizers, P3P, E-P3P, EPAL
Information Brokers	Infomediaries
Network-based	Proxies, Firewalls

Table 2 Olivier's (2003) classification of privacy technologies

Privacy technology category	Examples
Private communication	Cookie managers or blockers, encryption software
Anonymity	Anonymizers, Infomediaries
Personal Control	Ad blockers, P3P, Infomediaries, Proxies
Organizational safeguards	E-P3P, EPAL, Hippocratic Databases
Inference control	Privacy-preserving data mining

My proposal classifies privacy technologies according to *user behavioural phases*, that is, when the user

(1) Becomes Aware of privacy issues and rights,
(2) Acts to protect her/his privacy; note that Olivier's classification is a possible sub-classification for the Act phase of this Privacy Life Cycle Classification system.
(3) Detects privacy violations or potential privacy violations, and
(4) Resolves privacy conflicts.
(5) The lengths of time a user spends in each phase differs and the phases are cyclical, meaning that the user will re-enter them over time. These phases are illustrated in Fig. 1.

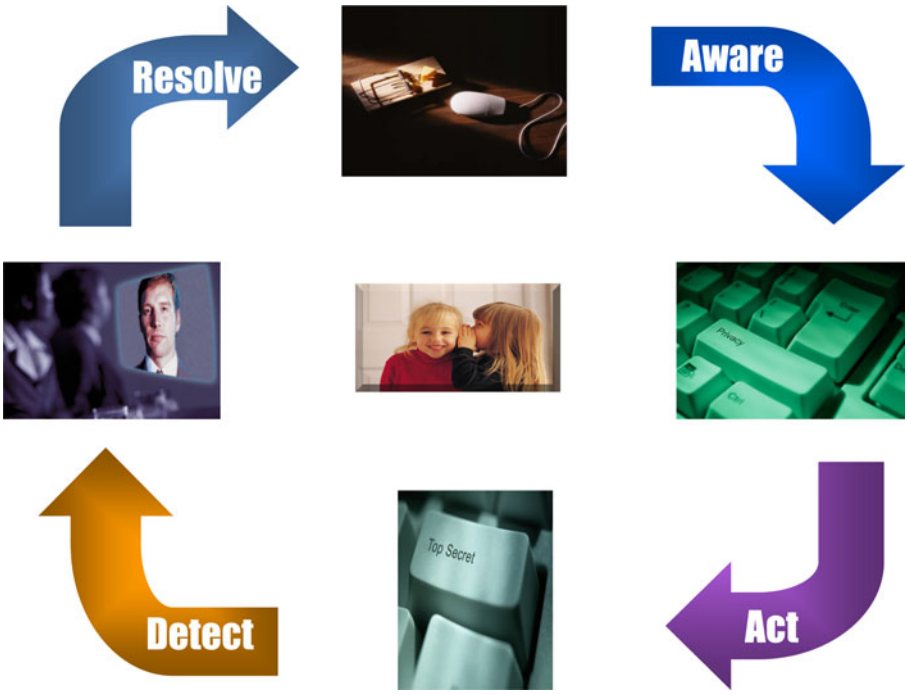

Fig. 1 Four phases of the user's online privacy life cycle

The design of layered privacy platforms for the mass increase of citizen's privacy-awareness is motivated by a platform layering strategy I observed as a best practice in value creation, via coupling platforms, from leading firms such as Salesforce and Google. In 2007, Google and Salesforce announced a partnership to connect their respective platforms so that Google's advertiser customers would be able to know on which web properties their advertisements were converting to leads and sales. Conversely, Salesforce's customers could directly facilitate moving the customer to the order phase, gain the added benefits of knowing what ads were engaging customers, and hence better manage ad campaign, lead, and order information. From a theoretical point of view, this coupling of Google and Salesforce platforms essentially connected the engage phase to the order phase of the customer life cycle (Craig and Jutla 2001). In terms of user control of her/his privacy, I identify the development and connection of the phases within a *privacy life cycle* shown in Fig. 1. Each phase can correspond to an individual privacy platform or integrate into one or more privacy platforms. Each phase can correspond to a category classification as per Table 3.

A privacy life cycle from the *user* perspective, to the best of my knowledge, has not been proposed before. In the literature, one finds privacy life cycles from the *organizational* perspective (Mont 2006; Guarda and Zannone 2009; Anton et al. 2004). These privacy life cycles for organizations focus on creating, maintaining, implementing and disposing of privacy policies, and monitoring employee and systems compliance to them. In common to both the user and organizational privacy life cycles are the information-providing and information-based services and the requirement to model personal data and support appropriate representations of user preferences. I further propose that the same phases of the privacy lifecycle provided from the *user* perspective can be used to classify the activities of the privacy life cycle from the *organizational* perspective. Details of the privacy life cycle from the organizational perspective are given in Jutla et al. 2010.

PrimeLife (2008) is a large European Initiative intending to create privacy technologies for the online arena. Areas of application include electronic commerce and social networks. Camenisch (2008), PrimeLife technical leader at IBM's Zurich Research Lab, states "We aim to develop a toolbox, which you could describe as an

Table 3 Life cycle-based classification of privacy technologies

Categories = phases of the privacy life cycle	Technology examples
Aware	P3P, PeCAN, web site resources
Act	Refrain from releasing selected private data (P3P, PeCAN), cookie managers, blockers, anonymizers, pseudonymizers, encryption software, firewalls, proxies, privacy-preserving data mining
Detect	Online access to personal data, De-anonymizing (linking) software
Resolve	Example Web sites: http://www.ipc.on.ca/english/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=8303, http://www.priv.gc.ca/cf-dc/index_e.cfm, http://www.privacyinternational.org/index.shtml, http://www.privacy.org.nz/court-cases/, http://www.cnil.fr/english/news-and-events/the-swift-case/,

integrated electronic 'data manager.' The data manager provides users with an overview of which personal data he or she uses when, where, and how. It lets users define default privacy settings and preferences for all kinds of applications, and it prompts the user if applications request data for any other purposes." Allowing users to define privacy settings and preferences for all kinds of applications implies that context mechanisms, similar to the concepts introduced in Bodorik and Jutla 2003, Jutla and Zhang (2005), Jutla and Bodorik (2005), and Jutla et al. (2006) for electronic commerce, will be supported. PrimeLife is a well-funded European project and its deliverables are expected to revolutionize available privacy technologies in the marketplace.

The PrimeLife initiative, as per a recent update on its application to social software (Kuczerawy et al. 2008), has not yet identified a platform solution for privacy as proposed in this paper. Rather Pekárek and Pötzsch (2009) examine privacy in social networks and provide use cases to specify privacy requirements for social network users. In Pekárek and Leenes's (2009) interesting position paper, researchers miss the fact that users can greatly influence the policies and practices of a social networking site. Further, the researchers have not identified that the strength of the business model of social networking sites depends on strong cross-side network effects wherein citizens comprise one side. User outrage will necessarily be avoided by the executive owners of these sites, and social networks will visibly try to accommodate user privacy needs once the users become aware and voice them.

Motivation for services proposed in this paper (e.g. in Tables 4 and 5) continues to appear in the literature. For example, Van Alsenoy et al (forthcoming) discuss whether privacy regulations should apply among users, and Reay et al. (2009) demonstrate how web sites are not necessarily visibly complying with jurisdictional privacy regulations.

The aware phase

PeCAN and P3P share a common privacy model based on an educational focus and *information-providing* approaches to enhancing user control over personally identifiable information. I present the argument that good mechanisms to provide user control, such as P3P, PeCAN and HCI- related privacy mechanisms, implicitly have an educational aspect to them. Indeed, electronic privacy research in the information systems, human-computer interaction, and computer science areas (Jajodia 1996; Kobsa 2002; Patrick and Kenny 2002), and various implementations (e.g. AT&T's Bird, Microsoft's IE6) encourage organizations to provide explanations to their customers for why and what purposes data is being collected and with whom the collected data can be shared. The rationale is that comprehension on the users'

Table 4 Six unique 2-way comparison services for user preferences, business policies, and government regulations

	Business	User	Government
Business	x		
User	x	x	
Government	x	x	x

Table 5 Ten complex privacy services

Comparison type	Entity	Entity	Entity
3-way comparisons (1 or more governments, 1 or more organizations, and 1 or more users)	Government	Organization	User
Multiple Orgs (2 or more)and 1 User	Organization	Organization	User
Multiple Governments (2 or more) and 1 User	Government	Government	User
Multiple Users (2 or more) and 1 Government	User	User	Government
Multiple Orgs (2 or more) and 1 Government	Organization	Organization	Government
Multiple Governments (2 or more)and 1 Org	Government	Government	Organization
Multiple Users (2 or more)and 1 Org	User	User	Organization
Multiple Governments (2 or more)	Government	Government	Government
Multiple Organizations (2 or more)	Organization	Organization	Organization
Multiple Users (2 or more)	User	User	User

part will prevent misunderstandings, increase the perception of user control, and hence increase trust in e-commerce.

P3P is foundational in that it provides a valuable XML vocabulary for privacy on which many information-providing services can be built. PeCAN expands P3P in two important ways (1) by allowing users to customize their privacy preferences according to contexts, and (2) providing sophisticated information-providing services that intend to help users avoid giving out information that can be used by others to harm their privacy.

While the Platform for Privacy Preferences (Cranor 2003; Cranor et al. 2002a, b, 2006) is the most mature online platform for making the user aware of what organizations' privacy policies state, its development may be complemented by other privacy platforms that are also information-and service providing. These complementary platforms may provide further sophisticated services to prevent the user from releasing private information, according to his/her privacy preferences, to an organization. This paper evolves the PeCAN (*Personal Context Agent Networking*) architecture into a platform and layers it onto the P3P platform, thereby illustrating how privacy services can develop and evolve in a platform environment. Moreover, a later section in this paper shows how the platform concept is a key vehicle for widespread user adoption of privacy web services.

Users' privacy requirements last a lifetime and beyond. Education is a first-phase preventative approach to privacy management. This first phase maps to the Aware phase of the user's online privacy life cycle illustrated in Fig. 1. Other phases are the Act, Detect, and Resolve phases. Each of these four phases are explained and illustrated in "The user's online privacy life cycle".

The act phase

User actions that emerge out of an increased privacy-awareness phase involve preventing privacy violations through limiting and/or avoiding release of private data to organizations, and questioning and/or negotiating with service providers about

their intentions regarding the management and use of the data before releasing it to organizations. These actions are win-win to users and business as empirical research results (Jutla et al. 2004b) show that adoption of *user intervention* (uIV) tools such as P3P-based agents, encryption, cookie cutters, pseudonymizers, and anonymizers increase user trust in e-business.

Using the PeCAN and P3P platforms, users can also actively choose not to reveal their personal data to requesting organizations and thus these platforms service the Act phase where users take action to protect their privacy through non-disclosure. However, non-disclosure is not always possible, and so other popular privacy technologies and tools have emerged for users to take further explicit action to protect their privacy. These include the encryption-based approaches found in the FaceCloak (Luo et al. 2009) and NOYB (Guha et al. 2008) services, the PGP encryption platform (PGP 2009), and GnuPG tools. Various forms of encryption have been used to address authentication, access control, data confidentiality, data integrity, and non-repudiation needs on secure networks for decades (Denning 1982; Jajodia 1996; You et al. 1998). Many users have sought encryption services when, for example, they look for the shttp or https prefixes in web URLs, or the lock symbol on web pages. Users employ encryption approaches at a later phase when they choose to take pragmatic action to secure their private data after becoming aware or educated about privacy risks and solutions.

In some popular online social networks, increasing the extent of encryption-based approaches may have the disadvantage of changing some degree of functionality of the social networks. The usability of the encryption techniques has been a complicating issue (Whitten and Tygar 1999). However, software developers are aware of the usability issues and hence encryption implementations are becoming friendlier and easier to use, as apparent in Google's Gmail support for SSL encryption.

Further, users can act to protect their privacy by employing anonymization technologies to prevent websites from collecting their identities by hiding or blocking identifying information such as cookies and IP addresses (Bayardo and Srikant 2003; Senicar et al. 2003; Goldberg et al. 1997). Other mature technical appliances for security and privacy that users actively employ are proxies and firewalls. Such tools are popularly described in the business literature (e.g. Panko 2008).

A popular means for a user to take control over maintaining her/his privacy is through applying the privacy settings available on browsers and some web sites. Social networking websites, in particular, are trying to address their users' privacy needs by providing settings to allow users to restrict certain categories of their private data from being displayed.

More emergent technologies are the location-based privacy protocols implemented in privacy services for mobile social networks, such as Buddy Beacon, Loopt, and Whrrl, and which are being prototyped (Zhong et al. 2007) in research labs. Moreover, attempts at identity theft can be prevented by user actively using web anti-spoofing tools. Web spoofing, also known as "phishing" or "carding", is a form of internet crime for identity theft (Chou et al. 2004). In Chou et al. (2004), a browser plug-in called *SpoofGuard* to protect users is described. The SpoofGuard detects spoofing by analyzing email to find suspicious links, and alerts the user.

The phases outlined here and the technologies discussed are from the *user* perspective and hence can be under the user control. Users benefit also from the *organizational* perspective when organizations similarly act and employ technologies to protect customer, employee, and partner privacy.

The detect phase

In the Detect phase, users may find out that their data has been mishandled in some way. For example, their information is aggregated in a manner that makes some private data visible and accessible to a larger audience than they initially intended. The violations can range from minor to severe. Users may detect privacy violations using many means including through simple online access of what data the organizations are holding and for what purposes the data were used. If these purposes, for instance, do not match what the user agreed to when her/his data was collected, then violations can be flagged.

Organizations and governments seek to preserve individuals' privacy while releasing information or profiling users to provide optimized services. A common approach is to de-identify data to be released by removing the identifiers. However, de-identified information can be recovered from existing information, i.e. the remaining data fields available about the user. This can lead to a type of inadvertent privacy violation known as a linkage attack where "attackers use innocuous data in one data set to identify a record in a second data set with both innocuous and sensitive data."(Greengard 2008)

Narayanan and Shmatikov (2009) created a re-identification algorithm that can be used to detect how private information is available online. Their algorithm re-identified users in the anonymized social network graphs available in social networking platforms by connecting the dots among user information provided on multiple platforms. The researchers showed how a third of the users, who can be verified to have accounts on Twitter and Flikr, were re-identified in the anonymous Twitter graph with a 12% error rate. Narayanan and Shmatikov (2009) also developed a re-identification algorithm that they applied to the Netflix Prize dataset, which contains anonymous movie ratings of 500,000 subscribers of Netflix, the world's largest online movie rental service. Using "the Internet Movie Database as the source of background knowledge, we successfully identified the Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information." (Narayanan and Shmatikov 2009) Note that identity-linking is not limited to social networks but can be done among pseudonyms or identifiers used to login, at the network-and application levels, on different systems, or email addresses, and so on.

It is possible that identity-linking can be the basis of a future user service as a user may find it useful to know what can be derived about him/her from the information posted on the web already. PeCAN also hosts a service for inference control (An et al. 2009) which prevents the user from releasing further information that would enable her/his privacy-sensitive contexts from being derived from those already released to ubiquitous software-enabled environments. In a sense PeCAN's inference control service does detection as it must first automatically detect a potential privacy violation and then alert the user to prevent it. It is a service that spans the Act and Detect phases.

Indeed, the services that provide users with reasonable control over their private information are information-based or information-providing. Similarly, the software services in firms that enforce the protection of customers and employee privacy are information-based or information-providing. Note that we can make a further distinction between information-based versus information-providing models. Encryption, anonymization, and anti-spoofing use *information-based* models in that they manipulate, perturb, or block information in some way and thus belong to one class, whereas technologies such as P3P, PeCAN, and re-identification are based on *information-providing* models.

The resolve phase

In the Resolve phase, users are provided with several options depending on their jurisdiction and its privacy governance models. In the US, recourse is through discussion, and if high-conflict, through user-actioned lawsuits. In countries with Privacy Commissioners, the user can complain to the Commissioner and any investigative and legal costs are borne by the government. Indeed, Bennett (1992) proposes five models that describe the privacy governance models in use by most countries' governments, according to who bears primary responsibility for protecting privacy interests: voluntary control (e.g. US), subject control (e.g. US), data commissioner model (e.g. Canada), registration (e.g.UK), and licensing (e.g. Norway). The bearer(s) of the primary responsibility are either or combinations of data gatherer, data subject, and government. In voluntary control and subject control, the organizations and citizens self-regulate on privacy issues. The data commissioner model uses a privacy ombudsman to help protect citizens' privacy. Whereas the registration and licensing models mean the data gatherers must first register with the government the data stores or databases which contain private data. Under the registration model, the government can deregister a store as a penalty if citizens complain about privacy infractions. In the licensing model, government employees are tasked to do inspections for compliance. Thus the privacy governance model also determines how active an oversight agency is in the Detect phase as well.

Many countries have web portals, blogs, and wikis to provide information leading to resolutions. The Canadian Federal Privacy Commissioner's web site has a serial listing of hundreds of privacy resolutions (Canada Federal Privacy Commissioner 2010). The Information and Privacy Commissioner of Ontario maintains a web site that includes indexed lookup of hundreds of summaries and resolutions (Ontario Information and Privacy Commissioner 2010). The online services for the Resolve phase are information-providing vs. transactional at this point.

Layering privacy platforms

Potentially there can be a privacy platform for each phase of the privacy life cycle, or one privacy platform can be created to host technologies to address all phases. It is more likely, in the beginning, with the fragmented efforts of privacy advocates, researchers, developers, and policymakers all around the world, that several platforms will emerge, and that the technologies to support the different user phases

will map to these platforms. Indeed, this fragmentation of privacy platforms is the phenomenon we are witnessing today.

The platform concept is central to the development of this paper. *A key concept is that online privacy services, which give the user some control over their private data, may be bundled in one or more privacy platforms and these privacy platforms may piggyback on social networking and other platform-mediated networks for widespread user adoption of privacy protection services*. The layered design illustrates this concept in Fig. 2.

A useful platform (e.g. Windows, Akamai) provides a subset of services and rules employed by users in most of their transactions. Further, successful platforms are characterized by their usability, convenience, and pervasiveness. Business researchers define the *platform-mediated network* (hereafter referred to as a *platform*) as providing "a subset of *components* and *rules* employed by users in most of their transactions." (Eisenmann et al. 2006) Examples of components are hardware, software, and services. *Rules* are the technical standards, protocols for information exchange, policies, and contracts that govern transactions (Baldwin and Clark 2000).

There are one-sided and many-sided platforms. In a one-sided platform, users are all part of a homogeneous user base whereas a many-sided platform supports different and non-overlapping groups or networks of users or customers. For example, in 2-sided networks (Rochet and Tirole 2003; Parker and Van Alstyne 2005), users are permanent members of one distinct group, a "side," which transacts with a second side. Examples of popular many-sided e-business platforms are

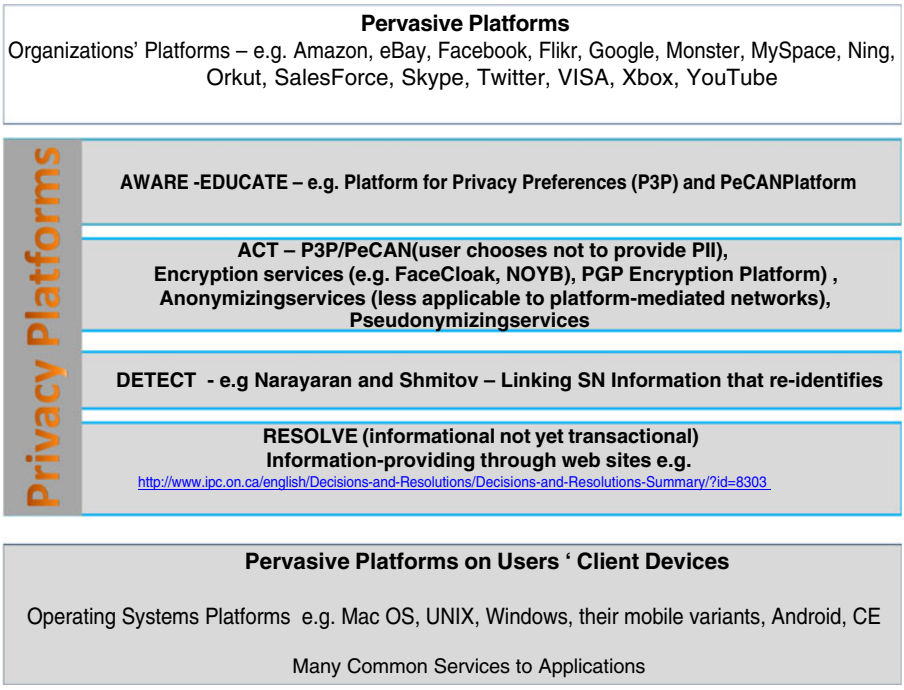

Fig. 2 Layering privacy platforms and operating systems and platform-mediated networks

Alibaba, Amazon, Baidu, eBay, Clipvn, SalesForce.com, Visa, Monster, Xbox, and YouTube while examples of many-sided online social networking platforms are Facebook, Flikr, Orkut, QQ,Ning, MySpace, and Twitter.

A platform's value to a user depends on the number of other network users, and is subject to network effects (Katz and Shapiro 1985; Economides 1996). Network effects represent users' willingness to participate in, as expressed as their willingness-to-pay to associate with a platform, in the presence of an increasing or decreasing number of participants in the networks mediated by the platform. Social networking sites enjoy strong same side and cross-side network effects. When many friends of a user join Facebook on the same-side, for example, the more valuable the platform becomes to the user as he/she can communicate conveniently with a larger number friends through a common medium. The more users that join Facebook, the more application developers (a second Facebook customer group), and advertisers (a third Facebook customer group) will join on the cross-side. Users value the variety offered by the larger application development group and hence the platform becomes more valuable to the users. The latter phenomenon is a cross-side effect in the direction of application group to the user. Details of the high-level layered platform design will be elaborated in "Layering platforms—P3P, PeCAN, operating systems, social networks, and others".

Layering platforms—P3P, PeCAN, operating systems, social networks, and others

This section provides an illustration of the design presented in "Layering privacy platforms". It details the layering and synergies of two privacy platforms for the Aware phase of the Privacy Life Cycle. The privacy platform design is then illustrated where the combined services of the two privacy platforms are sandwiched in between the operating systems on user devices, such as the iPhone, and social networks or other high-level platforms.

Platform for privacy preferences—P3P (1997–2007)

Developed from 1997–2007 by a relatively small group of experts from US and European universities and industry, the best-known online privacy platform is the Platform for Privacy Preferences (P3P). It enables organizations to represent their online privacy policies in a standard privacy-labeled format. Users' privacy software agents can then retrieve these specially formatted policies and automatically understand them. The syntax of P3P consists of a data schema and multiple privacy policy statements. The data schema part defines data elements that can be used in privacy policy statements. Each policy statement specifies what data will be collected, with whom they will be shared, for how long they will be retained and for what purposes. In order for the agents from the users' side to pre-fetch, interpret, and check these policies automatically, privacy policy statements are encoded in a machine-readable XML format on organizations' websites. The policy specification language has been a W3C Recommendation as P3P Version 1.0 since April 2002 (Cranor et al. 2002b), and P3P Version 1.1 is a Working group note as of 2007.

AT&T provides a free P3P agent called Privacy Bird as a user add-on to the IE6 browsers. Bird checks for P3P policies for all content on a page visited by the user, compares them to the users' privacy preferences, and reports on the match using a traffic-light metaphor (green, yellow, red), and a synopsis of alerts such a pop-up with text "this site can sell any medical data collected to third parties." In 2003, 30 percent of the top 100 Web sites were P3P enabled (Byers et al. 2003). In addition, a number of easy-to-use tools are available for Web-masters to post privacy policies in P3P format. Microsoft Internet Explorer 6 (IE6) and Netscape Navigator 7 Web browser provide basic P3P functionality. A 2002 study of mainly over 50-year old users reports that the Privacy Bird is a useful agent. These user privacy agents simplify the task of examining the privacy policies posted by the websites and determining whether they are acceptable to the users/clients—a task that is cumbersome and disliked by users according to Lorrie Cranor, a leading privacy researcher and P3P author.

The P3P 1.1 specification provides a full description of the industry-wide XML-based data schema for privacy as well as the P3P protocol. Their full descriptions can be found at w3c.org/p3p. Unfortunately, further work was suspended on the newest version of P3P (v 1.1.) in 2007, due to low browser uptake and industry response. As P3P provides the most useful privacy markup language for the web, progress for web privacy services and privacy-enabled semantic web services will be made if work continues on P3P 1.1 to move it to accepted W3C standard in the future, and for other sophisticated privacy services to be built on top of the P3P platform. An alternative option would be for P3P to be rebranded and incorporated in another platform. It is this author's opinion that low uptake of the use of P3P agents was directly due to:

(1) The lack of online privacy education for users in general, and hence a lack of user readiness to demand that companies carefully and ethically handle their private data in future,
(2) A lack of user awareness that such a platform was available, and
(3) The under-funding of research and development and marketing efforts to maintain and market the platform.

That future is still not here as the average online user is naïve, currently to the point of ignorance, regarding online privacy issues and how apparently "cool" or convenient platform services can violate her/his privacy. A more recent study (Cranor et al. 2008) shows that "P3P had been deployed on 10% of the sites returned in the top-20 results of typical searches, and on 21% of the sites returned in the top-20 results of e-commerce". However, we put ourselves in a good strategic and technical position to help address deficiencies and avert crises when privacy technology research is proactive and anticipative rather than reactive.

The PeCAN platform (2002–present)

PeCAN's platform vision is to provide common privacy services to other online platforms and e-businesses. PeCAN's common service provides *customized* privacy preferences according to user context (space, time, country, organization, role of person, role of other interacting persons). In contrast, P3P provides one set of privacy preferences for all contexts. In addition, PeCAN supports multiple privacy services. Examples are services to maintain privacy-contexts and user-control

mechanisms, sixteen enumerated services consisting of comparisons of government privacy regulations, business privacy policies, and user data handling preferences, and composite web services to maintain control over Personally Identifiable Information (PII) according to users' privacy and socio-economic concerns.

Software and services components of the PeCAN platform

PeCAN provides Web privacy services for managing users' social, ethical, and economic preferences for their private data. These services describe how the user can prevent the spread of their private information to unethical or environmentally unfriendly businesses, or to organizations that share customer data with a third party partner originating from a country with human rights abuses or poor privacy laws. Specifically, PeCAN's services can help users address the following socio-economic concerns.

➢A user wants to know whether her/his privacy preferences match the privacy practices of each of the organization's third party business partners.
➢A user wants to know whether privacy laws and authorities exist in Canada to enforce the intentions stated within the privacy policies on the businesses' web sites.
➢The user does not want to do business with a company that has CheatersInc or UnGreenCompany as a third party business partner because he/she considers these as unethical or environmentally unfriendly.
➢The user does not want to have her/his information shared with a third party business partner that is in a country with poor privacy laws.
➢The user does not want to deal with a company that shares customer data with a third party partner originating from a country with human rights abuses.

The PeCAN software agent architecture was presented in Jutla et al. 2006. It consists of a multi-agent system interacting with entities on behalf of the user. The platform prototype is developed in Java and C++ and uses mainstream web services standards, such as XML (Extensible Markup Language), SOAP, UDDI (Universal Description Discovery and Integration) , WSDL (Web Services Description Language), and the Web Ontology Language, OWL. Web privacy ontology (Kim et al. 2002) is a software component of PeCAN. It was motivated and designed in Jutla and Xu 2004; Jutla et al. 2006.

PeCAN's services support, among other things, a collaboration between its personal context agent (Jutla and Zhang 2005) and a P3P agent in order to apply context-specific privacy rules during a user's electronic commerce transaction with an organization's Web site or Web services. It has a number of other specialized software agents. A monitor agent (Bodorik and Jutla 2003; Jutla and Bodorik 2005) oversees the user's interaction with Web forms and other interaction mechanisms at Web service sites. A context agent manages dynamic changes of the user privacy context as the user interacts with sites on the Web, informs the user about the current privacy-related context for decision support within a Web transaction, and triggers revision of user privacy preferences either due to other agents in the architecture, or actions by the user. The arbitrator agent (He and Jutla 2006) allows users to negotiate on their PII's usage purposes, handling both recipients and retention periods of personally identifiable data with an organization on the Web. The

regulatory agent invokes privacy Web services and utilizes external service feeds and trusted third party (TTP) agents to obtain knowledge on privacy regulations, guidelines, and service sites in multiple jurisdictions. Recommendations for additions to P3P were made in Jutla and Xu (2004), Jutla et al. 2004a and Jutla and Bodorik (2005).

Other web privacy services can allow the user to find out more information about the privacy practices of an organization's business partners. Users are concerned as many companies share their data with partners and third party service providers. A user may be interested in examining a partner's privacy policy or finding out under which regulations and jurisdictions the partnering organizations fall. PeCAN supports a proof-of-concept ontological privacy service that can look up various countries' privacy regulations.

While the P3P agent compares a user's privacy preference and a business' privacy policy, a PeCAN service can compare a business and a government's privacy policy. Another PeCAN service would compare a user's privacy preferences and government privacy regulations. The six possible two-way comparison combinations are enumerated in Table 4.

Web privacy services are useful not only for enabling these six two-way comparisons among user, government, and business stakeholders, but also for single stakeholder comparisons. For example, a service to compare business policies can be useful in several areas. One is the area of multiple jurisdictions where users might deal with a Web multinational, that is, with a company doing electronic commerce through subsidiaries in many countries (for example Amazon Japan or Amazon UK). A Web service doing such a comparison would tap resources, such as the Safe Harbor initiative, which lists membership information of companies who abide by other countries' privacy laws when doing business in those countries. Another area could be a Web service in which a user can compare many business' privacy policies to determine which of them handle personally identifiable data in a manner that is appropriate to the user.

PeCAN provides a service to perform a *three-way comparison among user preferences, business practices, and government regulations* (Jutla and Xu 2004; Jutla et al. 2004a). This comparison could be useful to an Internet user in several ways. An automatic comparison between the contents of P3P elements representing business privacy practices and those representing privacy law may result in highlighting to the user (1) omissions in the business' P3P policy statements, or (2) concerns of mismatch of interpretation of privacy legislation. The P3P specification is not yet mature enough in terms of element definitions to handle many legal subtleties cleanly. Hence a Web service can be useful to the user in flagging absence/presence, or ambiguity, of fair information principles regarding privacy as defined in law in the business' practices expressed in P3P policies.

Table 5 enumerates several other useful services for PeCAN which are proposed in this paper, based on comparison services between businesses, governments, and users. That is, in future PeCAN can implement services for a user to compare the privacy policies of two or more businesses, the privacy regulations for two or more governments, two or more sets of user privacy preferences, the privacy policies of multiple businesses against a set of user privacy preferences, and so on.

A further PeCAN service makes context sharing among software agents privacy-conscious. Bayesian network-based inference control methods (An et al. 2006, 2009) prevent privacy-sensitive contexts from being derived from those already released to ubiquitous software-enabled environments.

To increase the usability of the web privacy services, and to bring privacy management to mobile voice commerce, in 2005, Keselj and Jutla developed a high-level conceptual multi-agent software architecture which integrates natural language capability to be used in Internet Information Retrieval (IIR) tasks and privacy management. These improved PeCAN services are at experimental stages.

The market sides of the PeCAN platform

The PeCAN architecture specifies software components and services that may run on standard computer hardware. Service transactions have specific workflow and user input requirements that are part of the platform rules. Rules for a privacy platform are also dictated by the jurisdiction(s) of the operating platforms, including country- and industry-relevant regulations, laws, and acts.

To evolve the PeCAN architecture to a platform, we identify its markets or sides. One market comprises the users with privacy concerns, including those whose socio-economic beliefs restrict the association of their privacy data with others, including organizations. The other market is composed of the organizations and their partners that wish to offer privacy protection to its users. See Fig. 3 for illustration of the two markets or sides to the PeCAN platform.

Some platform markets cannot be developed without piggybacking on other platforms. Such is the case with current privacy platforms. P3P and PeCAN's markets are limited without Internet Explorer, Safari, Mozilla Firefox, and Chrome's support for their P3P and PeCAN agents and services, and a privacy vocabulary that is a web standard. Each client device must have an operating system, and hence privacy platform dependence and layering on operating system platforms is a natural extension. Similarly, without organizations and application providers placing their privacy policies in P3P-markup format, existing privacy platforms, P3P and PeCAN, will not have another market with which to connect their user services.

In Fig. 3, I focused on layering P3P and PeCAN platforms with the social networking organizations' platforms as these hosts hundreds of millions of users in well over 180 countries. This paper thus proposes a strategy for stakeholders to use the strong network effects of the social networking (SN) platforms to make privacy services pervasive.

A platform can also be viewed as a technology disruptor. According to Brydon & Vining (2006), new technologies can disrupt a market by "changing individual incentives for creating and sharing information, raising or lowering the costs of enforcing property rights, reducing or relocating transaction costs, and supporting institutional mechanisms (e.g. rating/reputation systems)." I suggest that social networking platforms are ideal environments for institutionalizing privacy mechanisms as well. Such institutionalization would lead to pervasive provision and use of privacy services, and the enhancement of socially innovative platforms that have "assets which can hardly be copied and which contribute to sustainable competitiveness." (Scheinstock et al. 2001; Jutla and Yu 2008)

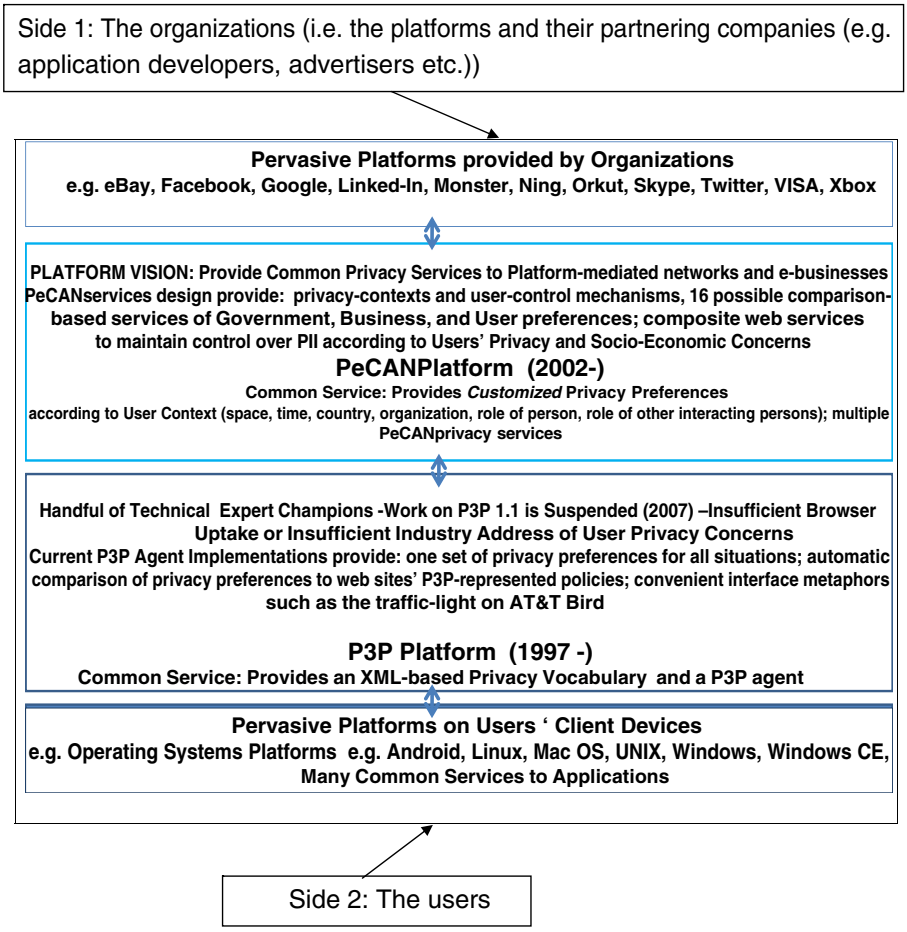

Fig. 3 Platform layers from operating systems on user devices to organizations' platforms

Technology research often anticipates a future scenario. In this case it would be a scenario where users are better educated about online privacy issues. Privacy training will come from multiple sources, including classes in schools and specialized courses for employees. It would be an oversight to overlook the social service that OSN platforms can provide to their users in helping build privacy awareness and promoting informed and forward-looking user choices.

User-centric combined services for the aware and act phases

Consider a user being logged on to an Online Social Network (OSN) site where she can not only communicate with friends and co-workers but also invoke widgets that enable her to bank, invest, pay bills, conduct e-commerce, donate to charity, volunteer, find an employer, recruit others, and so on. Each additional task supplies information to the OSN or its linked partners. Some of the information is personally

identifying. The user is in an uncertain environment where she has privacy, security, ethical, economic, and social concerns. Various issues that she may be concerned about may be a subset or a superset of the following:

(1) She wants to know all the intended purposes/uses and possible dissemination of her information which she has tagged as private at the OSN site.
(2) She wants to do business only with firms that post a privacy policy.
(3) She wants to know that the business' privacy practices match her privacy preferences and to be alerted if they do not.
(4) She wants a store that will not only encrypt her credit card information but also the contents of her shopping basket.
(5) She wants to know whether her privacy preferences match the privacy practices of each of the OSN supplier's third party business partners.
(6) She wants to know whether privacy laws and authorities exist in the business' jurisdiction to enforce the intentions stated within the privacy policies on the businesses' web sites.
(7) She does not want to do business with a company that has CheatersInc or UnGreenCompany as a third party business partner because she considers these as unethical or environmentally unfriendly.
(8) She does not want to have her information shared with a third party business partner that is in a country with poor privacy laws.
(9) She does not want to deal with a company that shares customer data with a third party partner originating from a country with human rights abuses.
(10) She wants to know which private data protection law has precedence for her transaction.
(11) She would like to negotiate a quick electronic contract with a third party partner of the OSN, in which the company becomes obligated to destroy her data if it and its assets are sold to another company.
(12) She wants to know that she does not inadvertently provide information on a Web form at this site that goes against her stated privacy preferences. For instance, she has a preference not to give out her age, but she provides her birth-date and weight in the context of buying prescription medication to a business linked to the OSN.
(13) When she returns to the OSN, she would like to review her information and contracts for all the businesses or organizations linked to the OSN.
(14) She wants to review her privacy preferences for a linked site when she returns to the OSN site.
(15) She wants to maintain online privacy preferences for particular classes of organizations.
(16) She wants the OSN to keep her data that she provides to its various partners unlinked.
(17) She wants to ensure that private data that she intends to give out will not cause her other private data to be derived.

Analyzing these requirements, we see that current P3P agents will support the first three requirements on this list. Requirement 4 can be satisfied by an extension to P3P with a <SAFEGUARDS> tag and accompanying extension of the P3P agent's matching algorithm to do a SAFEGUARDS comparison. Satisfying requirements 5–9

are the focus of the cooperating PeCAN Web services in (Jutla et al. 2004a). Data support in a Web privacy ontology combined with implementation of the PeCAN services shown in Tables 4 and 5 is envisaged to support requirement 10. Services to implement negotiation and contracts as in requirement 11 are described in another paper (He and Jutla 2006). PeCAN's design includes services to satisfy requirements 12–17.

State-of-the-art privacy agents, such as the P3P-based agent PrivacyBird (AT&T 2005), are currently limited by fixed-format form interfaces. User preferences are restricted to specifying user rules for handling of his/her personal data in categories such as health, financial, and physical data. A good example of such a form is the Privacy Preference Settings form that AT&T Bird uses (see www.privacybird.com/tour/1_2_beta/). These settings are done at a large grain level that is user-friendly but lacks flexibility for personalizing privacy software according to a wide range of subjective user preferences and weightings of these preferences.

It would be useful for these interfaces to be customizable to include other items such as:

- Warn me about companies that share customer information with other companies that do not have privacy statements.
- Warn me about companies that share with other companies whose practices violate my privacy, ethical, and/or social preferences.
- Warn me about a company that has a third party partner that is on my blocked list.
- Warn me about businesses, 3rd party, or otherwise, that are in jurisdictions with no enforcement of fair information practices.

Summary of contributions, managerial, and user implications

This paper introduces a privacy life cycle concept from the user perspective thereby contributing to the classification theory for online privacy management and technologies. The privacy life cycle of Aware, Act, Detect, and Resolve asserts at least the following:

(1) Users' knowledge of privacy issues and readiness to act on protecting privacy change over time and hence pass through different phases, each posing different challenges and opportunities in the changing online environment,
(2) Protecting privacy requires different, yet sometimes overlapping, strategies and tools in each life cycle stage, and
(3) Protecting a user's privacy continues indefinitely, so the phases will cycle or repeat continuously throughout her/his lifetime, and for those affected (e.g. family members), beyond the lifetime.

The second major contribution of the paper is a design for providing privacy protection via layering privacy platforms. The multi-layer privacy technology platforms and their services may map to one or more of the lifecycle phases. Formal privacy platforms from the user perspective currently exist only for the Aware and Act phases. Online technologies are becoming available to add to

platforms for the first three phases while the Resolve phase's technology assistance is mainly through information-providing web sites at this time. The paper illustrated the application of platform management theory (Eisenmann et al. 2006) to privacy platforms wherein the PeCAN architecture is evolved to a platform to show the value of layering and combining privacy services across privacy platforms. What user privacy requirements are addressed through the combined service offerings of the P3P and PeCAN platforms are identified.

Another key contribution is that the platform concept can be turned into a bonanza, versus a nightmare for privacy, as piggybacking a privacy platform onto the strong network effects of existing operating systems and social networking platforms could translate to wide scale adoption of privacy services for awareness, action, detection, and resolution. That is, a strategy to make privacy pervasive is for user privacy services to become widely available, predictably and consistently, across mainstream platforms. This paper proposed accomplishing the wide scale pervasiveness of privacy services through a design to layer privacy platforms onto existing popular platforms.

With a platform-based strategy, the popularity of social networks, and a growing suite of online privacy services to meet the needs of the phases of the privacy life cycle, in coming years billions of users will have access to and will adopt the tools to take control and maintain their privacy online.

References

An X, Jutla DN, Cercone N. Auditing and inference control for privacy preservation in uncertain environments. *First European Conference on Smart Sensing and Context*, Enschede, Netherlands, pp. 159–173; 2006.

An X, Jutla DN, Cercone N, Pluempitiwiriyawej C, Wang H. Uncertain inference control in privacy protection. Int J Inf Secur. 2009;8(6):423–31.

Anton AI, Bertino E, Li N, Yu T. A roadmap for comprehensive online privacy policy. Technical report, CERIAS, Purdue University, West Lafayette, CERIAS-2004-47; 2004.

AT&T PrivacyBird. http://www.privacybird.org/; 2005.

Baldwin C, Clark K. Design rules, Vol. 1: the power of modularity. Cambridge: MIT Press; 2000.

Bayardo RJ, Srikant R. Technological solutions for protecting privacy. Computer. 2003;36(9):115–8.

Bennett CJ. Regulating privacy: data protection and public policy in Europe and the United States. Ithaca: Cornell University Press; 1992.

Bodorik P, Jutla DN. Architecture for User Controlled e-Privacy. ACM Symposium on Applied Computing, Special Track on Electronic Commerce Technologies, Melbourne, Florida; 2003. p. 609–616.

Brydon M, Vining AR. Understanding the failure of internal knowledge markets: a framework for diagnosis and improvement. Inf Manage. 2006;43(2006):964–74.

Byers S, Cranor LF, Kormann DP. Automated analysis of P3P-enabled Web sites. *Proceedings of the 5th International Conference on Electronic Commerce*, Pittsburgh, Pennsylvania, USA, p. 326–338; 2003.

Camenisch J. Source: http://www.zurich.ibm.com/news/08/primelife.html; 2008.

Canada Federal Privacy Commissioner. http://www.priv.gc.ca/cf-dc/index_e.cfm; 2010.

Chou N, Ledesma R, Teraguchi Y, Mitchell JC. Client-side defense against web based identity theft. In *Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS'04)*, San Diego, CA, USA; 2004.

Craig J, Jutla DN. e-Business readiness: a customer-focused framework. Redwood City: Addison Wesley's Professional Information Technology Series; 2001.

Cranor FL. P3P: making privacy policies more useful. IEEE Security Privacy. 2003;2003:50–5.
Cranor LF, Egelman S, Sheng S, McDonald AM, Chowdhury A. P3P deployment on websites. *Electronic Commerce Research and Applications*. 2008;7(3):274–93.
Cranor LF, Guduru P, Arjula M. User interfaces for privacy agents. ACM Trans Comput-Hum Interact. 2006;13(2):135–78.
Cranor L, Langheinrich M, Marchiori M. A P3P preference exchange language 1.0 (APPEL 1.0). Technical report, W3C Working Draft, http://www.w3.org/TR/P3P-preference; 2002a.
Cranor L, Langheinrich M, Marchiori M, Presler-Marshall M, Reagle J. The platform for privacy preferences, 1.0 (P3P 1.0) specification. Technical report, W3C Recommendation, http://www.w3.org/TR/P3P; 2002b.
Denning D. Cryptography and data security. Addison-Wesley; 1982.
Economides N. The economics of networks. Int J Ind Econ. 1996;14:673–99.
Eisenmann T, Parker G, Van Alstyne M. Strategies for two-sided markets. *Harvard Business Review* Oct. 2006.
Facebook Statistics. Retrieved 18 Oct 2009, from http://www.facebook.com/press/info.php?statistics; 2009.
Greengard S. Privacy matters. CACM. 2008;51(9):17–8.
Goldberg I, Wagner D, Brewer EA. Privacy-enhancing technologies for the internet. In *Proceedings of the IEEE COMPCON'97*, p. 103–109, San Jose, CA, USA. IEEE Computer Society.
Guarda P, Zannone N. Towards the development of privacy-aware systems. Inf Softw Technol. 2009;51(2):337–50.
Guha S, Tang K, Francis P. NOYB: Privacy in online social networks. *Proceedings of the first workshop on online social networks*. Seattle, WA, USA. p. 49–54; 2008.
He Y, Jutla, DN. Contextual e-negotiation for the handling of private data in e-commerce on a semantic web. *Proceedings of the 39th Annual Hawaii International Conference on Systems Sciences*, 8 pages; 2006.
Jajodia S. Database security and privacy. ACM Comput Surv. 1996;28(1):129–31.
Jutla DN, Xu L. Privacy Agents and Ontology for the Semantic Web. Special Interest Group on Agent-based Information Systems, *Americas Conference on Information Systems*, New York City, USA, 10 pages; 2004.
Jutla DN, Bodorik P. Socio-technical architecture for online privacy. IEEE Security Privacy. 2005;3(2):29–39.
Jutla DN, Zhang Y. Maturing e-privacy with P3P and context agents. In *Proceedings of IEEE International Conference on E-Technology, E-Commerce and E-Service*, Hong Kong. p. 536–41; 2005.
Jutla DN, Yu W. Applying the Delta Model to mobile marketing management in the US marketplace. Int J Electron Bus, (IJEB). 2008;6(3):216–31.
Jutla DN, Bodorik P, Gao D. Management of private data: Web services addressing user privacy and economic, social, and ethical concerns. In: Jonker W, Petkovic M, editors. Secure Data Management: Proceedings of VLDB 2004 Workshop. Toronto: Springer-Verlag; 2004a. p. 100–17.
Jutla DN, Kelloway EK, Saifi S. Evaluation of user intervention tools for privacy on small and medium enterprises' online trust. In *Proceedings of IEEE Conference on Electronic Commerce (CEC'04)*, San Diego, CA. p. 281–288; 2004b.
Jutla DN, Bodorik P, Zhang Y. PeCAN: An architecture for user privacy and profiles in electronic commerce contexts on the Semantic Web. Inf Syst. 2006;31(4–5):295–320. Submitted for review on December 2003, Appeared online 2005.
Jutla D, Kanevsky D, Temkin A, An X, Matwin S. A classification system for online privacy technologies, Working Paper, FISMS-03-2010; 2010.
Katz M, Shapiro C. Network externalities, competition, and compatibility. Am Econ Rev. 1985;75:424–40.
Keselj V, Jutla DN. QTIP: Multi-Agent NLP and Privacy Architecture for Information Retrieval in Usable Web Privacy Software, *IEEE/WIC/ACM International Conference on Web Intelligence*, September 19–22, Copiegne, France, 2005, 7 pages; 2005.
Kim A, Joffman LJ, Martin CD. Building privacy into the semantic web: ontology needed now. *Semantic Web Workshop 2002*, Hawaii USA; 2002.
Kobsa A. Personalized hypermedia and international privacy, *Communications of the ACM, Special Issue on Adaptive Web Systems and Adaptive Hypermedia*. 45:5, p. 64–67; 2002.
Kuczerawy A, Pekárek M, Pötzsch S, Roosendaal A. Privacy and access control in social software. *PrimeLife Heartbeat 1.2.2*, November 2008.
Luo W, Xie Q, Hengartner U. FaceCloak: An Architecture for User Privacy on Social Networking Sites, IEEE International Conference on Information Privacy, Security, Risk and Trust, PASSAT, 2009, 8 pages.

Mont. On Privacy-Aware Information LifeCycle Management in Enterprises: Setting the Context. HP Laboratories and *ISSE 2006*. Rome, Italy; 2006.

Narayanan A, Shmatikov V. De-anonymizing Social Networks. In Proc. of *30th IEEE Symposium on Security and Privacy*, Oakland, CA, May 2009, pp. 173–187. IEEE Computer Society; 2009.

OECD. Inventory of privacy-enhancing technologies (PETs). Report DSTI/ICCP/REG (2001)1/FINAL, Working Party on Information Security and Privacy, Organisation for Economic Co-operation and Development; 2002.

Olivier MS. A layered architecture for privacy-enhancing technologies. S Afr Comput J. 2003;31:53–61.

Ontario Information and Privacy Commissioner. http://www.ipc.on.ca/english/Decisions-and-Resolutions/Decisions-and-Resolutions-Summary/?id=8303; 2010.

Panko R. Business data networks and telecommunications. Upper Saddle River: Prentice Hall; 2008.

Parker G, Van Alstyne M. Two-sided network effects: a theory of information product design. Manage Sci. 2005;51:1494–504.

Patrick A, Kenny S. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions, July 2002, available at http://www.iit.nrc.ca/~patricka/legint/from_legislation_to_interface.pdf, viewed on July 2002.

Pekárek M, Leenes R. Privacy and Social Network Sites: Follow the Money! Position Paper for the *W3C Workshop on the Future of Social Networking*, Barcelona, January 15–16, 2009.

Pekárek M, Pötzsch S. Requirements and concepts for privacy-enhancing access control in social networks and collaborative Workspaces, *PrimeLife Heartbeat 1.2.5*, http://www.primelife.eu/images/stories/deliverables/h1.2.5-requirements_selective_access_control-public.pdf; 2009.

PGP. The PGP Encryption Platform - http://www.pgp.com/products/platform/index.html; 2009.

Reay I, Dick S, Miller J. A large-scale empirical study of P3P privacy policies: Stated actions vs. legal obligations *ACM Transactions on the Web (TWEB)*, Volume 3, Issue 2; 2009.

Rochet, JC, Tirole J. Platform Competition in two-sided markets. JEEA 2003;1(4):990–1029.

Scheinstock G, Hamalainen T. Transformation of the Finnish innovation system: A network approach, *SITRA Series*, 7, Helsinki, 2001.

Senicar V, Jerman B, Klobucar T. Privacy-enhancing technologies - approaches and development. Comput Stand Interfaces. 2003;25:147–58.

Van Alsenoy B, Ballet J, Kuczerawy A. Social networks and web 2.0: are users also bound by data protection regulations?; forthcoming.

Whitten A, Tygar JD. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium*, p. 169–84. Usenix, 1999.

You CH, Zhou J, Lam K-Y. On the efficient implementation of fair non-repudiation, ACM SIGCOMM Computer Communication Review 28:5; 1998, p. 50–60.

Zhong G, Goldberg I, Hengartner U. Louis, Lester and Pierre: Three Protocols for Location Privacy. *Proc. of Seventh Privacy Enhancing Technologies Symposium (PETS 2007)*, Ottawa, ON, Canada; June 2007, p. 62–76.